Docket No. 246433US2RD/ims

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Hiroshi ISOZAKI, et al.

GAU:

SERIAL NO: 10/729,964

EXAMINER:

FILED: December 9, 2003

FOR: CONTENTS TRANSMISSION/RECEPTION SCHEME WITH FUNCTION FOR LIMITING RECIPIENTS

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of **35 U.S.C. §120**.

☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of **35 U.S.C. §119(e)**: **Application No.** **Date Filed**

☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of **35 U.S.C. §119**, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

COUNTRY	**APPLICATION NUMBER**	**MONTH/DAY/YEAR**
JAPAN	2002-357168	December 9, 2002

Certified copies of the corresponding Convention Application(s)

☒ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

☐ were filed in prior application Serial No. filed

☐ were submitted to the International Bureau in PCT Application Number
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and

☐ (B) Application Serial No.(s)

☐ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Marvin J. Spivak
Registration No. 24,913

Joseph A. Scafetta, Jr.
Registration No. 26, 803

Customer Number
22850
Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 05/03)

10/729,964
T654

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００２年１２月　９日

出願番号
Application Number: 特願２００２－３５７１６８

[ST. 10/C]: [ＪＰ２００２－３５７１６８]

出願人
Applicant(s): 株式会社東芝

２００３年　７月１８日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０５７４４６

【書類名】　特許願

【整理番号】　14003301

【提出日】　平成14年12月 9日

【あて先】　特許庁長官殿

【国際特許分類】　H04B 7/26

【発明の名称】　コンテンツ送受信システム、コンテンツ送信装置、コンテンツ受信装置及びコンテンツ送受信方法

【請求項の数】　21

【発明者】

【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

【氏名】　磯崎　宏

【発明者】

【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

【氏名】　石原丈士

【発明者】

【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

【氏名】　小堺康之

【発明者】

【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

【氏名】　斉藤　健

【特許出願人】

【識別番号】　000003078

【住所又は居所】　東京都港区芝浦一丁目１番１号

【氏名又は名称】　株式会社　東　芝

【代理人】

【識別番号】　100075812

【弁理士】

【氏名又は名称】　吉　武　賢　次

【選任した代理人】

【識別番号】　100088889

【弁理士】

【氏名又は名称】　橘　谷　英　俊

【選任した代理人】

【識別番号】　100082991

【弁理士】

【氏名又は名称】　佐　藤　泰　和

【選任した代理人】

【識別番号】　100096921

【弁理士】

【氏名又は名称】　吉　元　弘

【選任した代理人】

【識別番号】　100103263

【弁理士】

【氏名又は名称】　川　崎　康

【先の出願に基づく優先権主張】

【出願番号】　特願2002-313300

【出願日】　平成14年10月28日

【手数料の表示】

【予納台帳番号】　087654

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　0102514

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　コンテンツ送受信システム、コンテンツ送信装置、コンテンツ受信装置及びコンテンツ送受信方法

【特許請求の範囲】

【請求項１】

送信装置と、この送信装置からコンテンツを受信する少なくとも１台の受信装置と、を備えたコンテンツ送受信システムにおいて、

前記送信装置は、

コンテンツ送信要求を行った前記受信装置との間で、認証・鍵交換処理を行う第１の認証・鍵交換処理手段と、

前記受信装置の機器識別情報を送信するよう前記受信装置に対して機器識別情報要求を送信する機器識別情報送信要求手段と、

前記受信装置から送信された前記機器識別情報を登録する機器識別情報登録手段と、

前記受信装置のIP（Internet Protocol）アドレスに対応する前記機器識別情報を、前記受信装置が接続されているネットワークから検索する機器識別情報検索手段と、

前記検索された機器識別情報と前記機器識別情報登録手段に登録されている機器識別情報とが一致するか否かを判定する比較判定手段と、

前記比較判定手段による一致判定結果に応じて、コンテンツ送信要求を行った前記受信装置へのコンテンツの配布条件を変更する配布条件決定手段と、を有し、

前記受信装置は、

前記送信装置に対して前記コンテンツ送信要求を行うコンテンツ送信要求手段と、

前記送信装置からの前記機器識別情報要求を受信すると、自装置の前記機器識別情報を前記送信装置に送信する機器識別情報送信手段と、を有することを特徴とするコンテンツ送受信システム。

【請求項２】

前記機器識別情報は、ネットワークインタフェースのMACアドレスであり、

前記機器識別情報検索手段は、前記受信装置のIPアドレスをキーとするMACアドレス検索要求を、前記受信装置が接続されるイーサネット（登録商標）セグメントに送信するとともに、MACアドレス検索結果を受信することを特徴とする請求項１に記載のコンテンツ送受信システム。

【請求項３】

前記機器識別情報検索手段は、ARPにより、前記受信装置のIPアドレスから対応するMACアドレスを検索することを特徴とする請求項２に記載のコンテンツ送受信システム。

【請求項４】

前記第１の認証・鍵交換処理手段は、DTCP（Digital Transmission Contents Protection）による認証・鍵交換処理を行うことを特徴とする請求項１及至３のいずれかに記載のコンテンツ送受信システム。

【請求項５】

前記機器識別情報送信手段は、MACアドレスに電子署名を添付して前記送信装置に送信することを特徴とする請求項３または４に記載のコンテンツ送受信システム。

【請求項６】

前記送信装置は、MACアドレスに電子署名が添付されている場合には、当該MACアドレスが改ざんされているか否かを検証する検証手段を有し、

前記機器識別情報登録手段は、前記検証手段により改ざんされていないと判断された場合のみ、当該MACアドレスを登録することを特徴とする請求項５に記載のコンテンツ送受信システム。

【請求項７】

前記受信装置は、

前記送信装置との間で認証・鍵交換処理を行う第２の認証・鍵交換処理手段と、

前記送信装置から暗号化されたコンテンツを受信するネットワークインタフェース手段と、

前記受信された暗号化されたコンテンツを、前記第２の認証・鍵交換処理手段で交換された鍵を用いて復号を行う暗号処理手段と、を有することを特徴とする請求項１及至６のいずれかに記載のコンテンツ送受信システム。

【請求項８】

少なくとも１台の受信装置に対してコンテンツを送信するコンテンツ送信装置において、

コンテンツ送信要求を行った前記受信装置との間で、認証・鍵交換処理を行う認証・鍵交換処理手段と、

前記受信装置の機器識別情報を送信するよう前記受信装置に対して機器識別情報要求を送信する機器識別情報送信要求手段と、

前記受信装置から送信された前記機器識別情報を登録する機器識別情報登録手段と、

前記受信装置のIPアドレスに対応する前記機器識別情報を、前記受信装置が接続されているネットワークから検索する機器識別情報検索手段と、

前記検索された機器識別情報と、前記機器識別情報登録手段に登録されている機器識別情報と、が一致するか否かを判定する比較判定手段と、

前記比較判定手段による一致判定結果に応じて、コンテンツ送信要求を行った前記受信装置へのコンテンツの配布条件を変更する配布条件決定手段と、を備えることを特徴とするコンテンツ送信装置。

【請求項９】

送信装置からのコンテンツを受信するコンテンツ受信装置において、

前記送信装置に対してコンテンツ送信要求を行うコンテンツ送信要求手段と、

コンテンツ送信要求先である前記送信装置との間で、認証・鍵交換処理を行う認証・鍵交換処理手段と、

前記送信装置の機器識別情報を送信するよう前記送信装置に対して機器識別情報要求を送信する機器識別情報送信要求手段と、

前記送信装置から送信された前記送信装置の機器識別情報を登録する機器識別情報登録手段と、

前記送信装置のIPアドレスに対応する前記機器識別情報を、前記送信装置が接

続されているネットワークから検索する機器識別情報検索手段と、

前記検索された機器識別情報と、前記機器識別情報登録手段に登録されている機器識別情報と、が一致するか否かを判定する比較判定手段と、

前記比較判定手段による一致判定結果に応じて、コンテンツ送信要求先である前記送信装置からのコンテンツ配布条件を決定する配布条件決定手段と、を備えることを特徴とするコンテンツ受信装置。

【請求項１０】

送信装置と、この送信装置からコンテンツを受信する少なくとも１台の受信装置と、を備えたコンテンツ送受信システムにおいて、

前記受信装置は、

前記送信装置に対してコンテンツ送信要求を行うコンテンツ送信要求手段と、

コンテンツ送信要求先である前記送信装置との間で、認証・鍵交換処理を行う第１の認証・鍵交換処理手段と、

前記送信装置の機器識別情報を送信するよう前記送信装置に対して機器識別情報要求を送信する機器識別情報送信要求手段と、

前記送信装置から送信された前記送信装置の機器識別情報を登録する機器識別情報登録手段と、

前記送信装置のIPアドレスに対応する前記機器識別情報を、前記送信装置が接続されているネットワークから検索する機器識別情報検索手段と、

前記検索された機器識別情報と、前記機器識別情報登録手段に登録されている機器識別情報と、が一致するか否かを判定する比較判定手段と、

前記比較判定手段による一致判定結果に応じて、コンテンツ送信要求先である前記送信装置からのコンテンツ配布条件を決定する配布条件決定手段と、を有し、

前記送信装置は、

前記受信装置からの前記機器識別情報要求を受信すると、自装置の前記機器識別情報を前記受信装置に送信する機器識別情報送信手段と、

コンテンツ送信要求を行った前記受信装置との間で、認証・鍵交換処理を行う第２の認証・鍵交換処理手段と、

前記配布条件決定手段で決定された配布条件に従って、コンテンツの送信制御を行うコンテンツ送信制御手段と、を有することを特徴とするコンテンツ送受信システム。

【請求項１１】

送信装置からのコンテンツを受信可能なコンテンツ受信装置において、

前記送信装置から自装置の機器識別情報検索要求があったか否かを判定する機器識別情報検索判定手段と、

前記機器識別情報検索判定手段により前記機器識別情報検索要求がなかったと判定された場合には、前記送信装置からのコンテンツの受信を禁止するコンテンツ受信制御手段と、を備えることを特徴とするコンテンツ受信装置。

【請求項１２】

前記送信装置から自装置の機器識別情報の送信要求があった場合に、前記機器識別情報及び機器識別情報の検索事前通知応答を前記送信装置に送信する自装置情報送信手段を備えることを特徴とする請求項１１に記載のコンテンツ受信装置。

【請求項１３】

少なくとも１台の受信装置に対してコンテンツを送信可能なコンテンツ送信装置において、

前記受信装置に対して、該受信装置の機器識別情報検索を事前通知する事前通知手段と、

前記受信装置のIPアドレスに対応する前記機器識別情報を、前記受信装置が接続されているネットワークから検索する機器識別情報検索手段と、

前記受信装置から送信された前記機器識別情報を登録する機器識別情報登録手段と、

前記機器識別情報検索手段で検索された機器識別情報と、前記機器識別情報登録手段に登録された機器識別情報と、が一致するか否かを判定する比較判定手段と、

前記受信装置から送信された、前記機器識別情報検索の事前通知に対する応答を受信したか否かを判定する要求応答受信判定手段と、

前記比較判定手段及び前記要求応答受信判定手段による判定結果に基づいて、前記受信装置へのコンテンツの配布条件を決定する配布条件決定手段と、を備えることを特徴とするコンテンツ送信装置。

【請求項１４】

送信装置と、この送信装置からコンテンツを受信する少なくとも１台の受信装置と、を備えたコンテンツ送受信システムにおいて、

前記送信装置は、

前記受信装置に対して、該受信装置の機器識別情報検索を事前通知する事前通知手段と、

前記受信装置のIPアドレスに対応する前記機器識別情報を、前記受信装置が接続されているネットワークから検索する機器識別情報検索手段と、

前記受信装置から送信された前記機器識別情報を登録する機器識別情報登録手段と、

前記機器識別情報検索手段で検索された機器識別情報と、前記機器識別情報登録手段に登録された機器識別情報と、が一致するか否かを判定する比較判定手段と、

前記機器識別情報検索の事前通知に対する応答を受信したか否かを判定する要求応答受信判定手段と、

前記比較判定手段及び前記要求応答受信判定手段による判定結果に基づいて、前記受信装置へのコンテンツの配布条件を決定する配布条件決定手段と、を有し、

前記受信装置は、

前記送信装置からの前記機器識別情報要求を受信すると、自装置の前記機器識別情報及び機器識別情報の検索事前通知応答を前記送信装置に送信する自装置情報送信手段を有することを特徴とするコンテンツ送受信システム。

【請求項１５】

少なくとも１台の受信装置に対してコンテンツを送信可能なコンテンツ送信装置において、

前記受信装置から自装置の機器識別情報検索要求があったか否かを判定する機

器識別情報検索判定手段と、

前記機器識別情報検索判定手段により前記機器識別情報検索要求がなかったと判定された場合には、前記受信装置へのコンテンツの送信を禁止するコンテンツ送信制御手段と、を備えることを特徴とするコンテンツ送信装置。

【請求項１６】

送信装置からのコンテンツを受信するコンテンツ受信装置において、

前記送信装置に対して、該送信装置の機器識別情報検索を事前通知する事前通知手段と、

前記送信装置に対してコンテンツ送信要求を行うコンテンツ送信要求手段と、

コンテンツ送信要求先である前記送信装置との間で、認証・鍵交換処理を行う認証・鍵交換処理手段と、

前記送信装置の機器識別情報を送信するよう前記送信装置に対して機器識別情報要求を送信する機器識別情報送信要求手段と、

前記送信装置から送信された前記送信装置の機器識別情報を登録する機器識別情報登録手段と、

前記送信装置のIPアドレスに対応する前記機器識別情報を、前記送信装置が接続されているネットワークから検索する機器識別情報検索手段と、

前記検索された機器識別情報と、前記機器識別情報登録手段に登録されている機器識別情報と、が一致するか否かを判定する比較判定手段と、

前記比較判定手段による一致判定結果に応じて、コンテンツ送信要求先である前記送信装置からのコンテンツ配布条件を決定する配布条件決定手段と、を備えることを特徴とするコンテンツ受信装置。

【請求項１７】

送信装置と、この送信装置からコンテンツを受信する少なくとも１台の受信装置と、を備えたコンテンツ送受信システムにおいて、

前記送信装置は、

前記受信装置から自装置の機器識別情報検索要求があったか否かを判定する機器識別情報検索判定手段と、

前記機器識別情報検索判定手段により前記機器識別情報検索要求がなかったと

判定された場合には、前記受信装置へのコンテンツの送信を禁止するコンテンツ送信制御手段と、を有し、

前記受信装置は、

前記送信装置に対して、該送信装置の機器識別情報検索を事前通知する事前通知手段と、

前記送信装置に対してコンテンツ送信要求を行うコンテンツ送信要求手段と、

コンテンツ送信要求先である前記送信装置との間で、認証・鍵交換処理を行う認証・鍵交換処理手段と、

前記送信装置の機器識別情報を送信するよう前記送信装置に対して機器識別情報要求を送信する機器識別情報送信要求手段と、

前記送信装置から送信された前記送信装置の機器識別情報を登録する機器識別情報登録手段と、

前記送信装置のIPアドレスに対応する前記機器識別情報を、前記送信装置が接続されているネットワークから検索する機器識別情報検索手段と、

前記検索された機器識別情報と、前記機器識別情報登録手段に登録されている機器識別情報と、が一致するか否かを判定する比較判定手段と、

前記比較判定手段による一致判定結果に応じて、コンテンツ送信要求先である前記送信装置からのコンテンツ配布条件を決定する配布条件決定手段と、を有することを特徴とするコンテンツ送受信システム。

【請求項１８】

送信装置と、この送信装置からコンテンツを受信する少なくとも１台の受信装置と、を備えたコンテンツ送受信方法において、

前記送信装置は、

コンテンツ送信要求を行った前記受信装置との間で、認証・鍵交換処理を行い、

前記受信装置の機器識別情報を送信するよう前記受信装置に対して機器識別情報要求を送信し、

前記受信装置から送信された前記機器識別情報を機器識別情報登録テーブルに登録し、

前記受信装置のIP（Internet Protocol）アドレスに対応する前記機器識別情報を、前記受信装置が接続されているネットワークから検索し、

前記検索された機器識別情報と前記機器識別情報登録テーブルに登録されている機器識別情報とが一致するか否かを判定し、

一致するか否かの判定結果に応じて、コンテンツ送信要求を行った前記受信装置へのコンテンツの配布条件を変更し、

前記受信装置は、

前記送信装置に対して前記コンテンツ送信要求を行い、

前記送信装置からの前記機器識別情報要求を受信すると、自装置の前記機器識別情報を前記送信装置に送信することを特徴とするコンテンツ送受信方法。

【請求項１９】

送信装置と、この送信装置からコンテンツを受信する少なくとも１台の受信装置と、を備えたコンテンツ送受信方法において、

前記受信装置は、

前記送信装置に対してコンテンツ送信要求を行い、

コンテンツ送信要求先である前記送信装置との間で、認証・鍵交換処理を行い、

前記送信装置の機器識別情報を送信するよう前記送信装置に対して機器識別情報要求を送信し、

前記送信装置から送信された前記送信装置の機器識別情報を機器識別情報登録テーブルに登録し、

前記送信装置のIPアドレスに対応する前記機器識別情報を、前記送信装置が接続されているネットワークから検索し、

前記検索された機器識別情報と、前記機器識別情報登録手段に登録されている機器識別情報と、が一致するか否かを判定し、

一致するか否かの判定結果に応じて、コンテンツ送信要求先である前記送信装置からのコンテンツ配布条件を決定し、

前記送信装置は、

前記受信装置からの前記機器識別情報要求を受信すると、自装置の前記機器識

別情報を前記受信装置に送信し、

コンテンツ送信要求を行った前記受信装置との間で、認証・鍵交換処理を行い、

前記決定された配布条件に従って、コンテンツの送信制御を行うことを特徴とするコンテンツ送受信方法。

【請求項２０】

送信装置と、この送信装置からコンテンツを受信する少なくとも１台の受信装置と、を備えたコンテンツ送受信システムにおいて、

前記送信装置は、

前記受信装置に対して、該受信装置の機器識別情報検索を事前通知する事前通知手段と、

前記受信装置のIPアドレスに対応する前記機器識別情報を、前記受信装置が接続されているネットワークから検索する機器識別情報検索手段と、

前記受信装置から送信された前記機器識別情報を登録する機器識別情報登録手段と、

前記機器識別情報検索手段で検索された機器識別情報と、前記機器識別情報登録手段に登録された機器識別情報と、が一致するか否かを判定する比較判定手段と、

前記比較判定手段及び前記要求応答受信判定手段による判定結果に基づいて、前記受信装置へのコンテンツの配布条件を決定する配布条件決定手段と、を有し、

前記受信装置は、

前記送信装置から自装置の機器識別情報検索要求があったか否かを判定する機器識別情報検索判定手段と、

前記機器識別情報検索判定手段により前記機器識別情報検索要求がなかったと判定された場合には、前記送信装置からのコンテンツの受信を禁止するコンテンツ受信制御手段と、を有することを特徴とするコンテンツ送受信方法。

【請求項２１】

送信装置と、この送信装置からコンテンツを受信する少なくとも１台の受信装

置と、を備えたコンテンツ送受信方法において、

前記送信装置は、

前記受信装置から自装置の機器識別情報検索要求があったか否かを判定し、

前記機器識別情報検索要求がなかったと判定された場合には、前記受信装置へのコンテンツの送信を禁止し、

前記受信装置は、

前記送信装置に対して、該送信装置の機器識別情報検索を事前通知し、

前記送信装置に対してコンテンツ送信要求を行い、

コンテンツ送信要求先である前記送信装置との間で、認証・鍵交換処理を行い、

前記送信装置の機器識別情報を送信するよう前記送信装置に対して機器識別情報要求を送信し、

前記送信装置から送信された前記送信装置の機器識別情報を登録し、

前記送信装置のIPアドレスに対応する前記機器識別情報を、前記送信装置が接続されているネットワークから検索し、

前記検索された機器識別情報と、前記機器識別情報登録手段に登録されている機器識別情報と、が一致するか否かを判定し、

一致するか否かの判定結果に応じて、コンテンツ送信要求先である前記送信装置からのコンテンツ配布条件を決定することを特徴とするコンテンツ送受信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、送信装置から受信装置にコンテンツを送信するコンテンツ送受信システム、コンテンツを送信するコンテンツ送受信システム、コンテンツ送信装置、コンテンツ受信装置及びコンテンツ送受信方法に関する。

【０００２】

【従来の技術】

近年の計算機ネットワークの普及やデジタル化に伴い、デジタル情報家電と呼

ばれる製品が普及しつつある。また、地上波デジタル放送の開始に伴い、デジタル放送対応のテレビ、セットトップボックス及びDVDレコーダ等が、今後より一層普及することが予想される。これらのデジタル家電がネットワークで接続されれば利用者にとって有益である。

【０００３】

このようなデジタルコンテンツは、劣化することなく容易に複製できるという利点を持つ反面、コンテンツの著作権に関して注意を払わなければならない。

【０００４】

図３３は送信装置と受信装置を備えた従来のネットワークシステムの全体構成を示すブロック図である。図３３に示すように、本発明に係る送信装置１（以下ソース機器Ｂと呼ぶ）は、イーサネット等のローカルエリアネットワーク２に接続されている。このローカルエリアネットワーク２のイーサネットセグメントＡ３には、ソース機器Ｂ１、受信装置４（以下シンク機器Ａと呼ぶ）及びルーター機器Ｃ５が接続されている。ルーター機器Ｃ５には、インターネット６を介してシンク機器Ｄ７が接続されている。シンク機器Ａ４は、ソース機器Ｂ１からローカルエリアネットワーク２を経由してコンテンツを受信する。一方、シンク機器Ｄ７は、ルータ機器Ｃ５とインターネット６を経由してソース機器Ｂ１と通信可能な範囲に位置する。

【０００５】

ここで、コンテンツとは、例えばMPEG4データのような動画データや音声データ、またはテキストデータや画像データのようなドキュメントなどのデジタルコンテンツを指す。ここでは、説明を簡単にするため、著作権保護をかけた上で転送すべきデジタルコンテンツ（以下、単にコンテンツを呼ぶ）を念頭に置く。

【０００６】

ここで、ソース機器Ｂ１からシンク機器Ａ４とシンク機器Ｄ７にコンテンツを送信する場合を考える。この時、注意すべきはコンテンツの著作権である。前述したように、当該コンテンツをやり取りする範囲は、一定の範囲内、例えば、著作権３０条の私的使用の範囲内などの正当な権限の範囲内、あるいはそれよりもさらに狭い範囲内に制限され、その範囲を超えて、例えば他人間でのコンテンツ

のやりとりはできないようにすることが望ましい。

【０００７】

そこで、著作権保護を行うために、図３３のネットワークシステムにおけるコンテンツの転送に関し、次の規則を用いることとする。

【０００８】

（１）ローカルエリアネットワーク内では、著作権保護を行うべきコンテンツの送受信を許可する。なぜならば、ローカルエリアネットワークに接続された機器であれば、個人や家庭内で楽しむ範囲での通信であるとみなすことができるからである。

【０００９】

（２）ローカルエリアネットワーク外では、著作権保護を行うべきコンテンツの送受信を許可しない。ローカルエリアネットワーク外での通信とは、例えば図３３に示すソース機器Ｂ１とシンク機器Ｄ７との通信など、インターネットや電話網等の公衆網を介したオープンな通信を示す。なぜならば、ローカルエリアネットワークに閉じない通信は、個人あるいは家庭内で楽しむ範囲の通信とみなすことができないからである。

【００１０】

なお、以下では、一例としてローカルエリアネットワークとしてイーサネットを用い、上位レイヤーでのコンテンツの送受信にIP（Internet Protocol）を用いるものとする。IPについては、例えばhttp://www.ietf.orgにて取得可能な文献に詳しく記載されている。もちろん、その他のプロトコル、例えばローカルエリアネットワークがIEEE1394で構成されており、上位レイヤーとしてIPをエミュレーションしたIP over 1394であってもよい。

【００１１】

コンテンツの配布範囲を個人が楽しむ範囲内に限定するための1つの方法として、同一イーサネットセグメント内に限定した通信のみに許可する方法が考えられる。これを実現するため、従来では、例えば、（１）イーサネットパケットでAKEを行う方法（特許文献１参照）、（２）送受信の機器のネットワークアドレスが同一であるか確認する方法（特許文献２参照）などが提案されている。他に

も、（３）TTL（Time To Field）を１にセットしてIPパケットを送信する方法、（４）それらを組み合わせた方法などがある。

【００１２】

図３４で示した環境において、ソース機器Ｂ１からシンク機器へのコンテンツの送受信を同一イーサネットセグメント間に限定するために、（２）と（３）の方法を組み合わせた方法を一例として以下に示す。

【００１３】

一般的には、IPにおいて、複数の機器のネットワークアドレスが同一であれば、同一のイーサネットセグメントに所属すると考えられるため、ソース機器Ｂ１とシンク機器のネットワークアドレスが同一であることを確認すれば、双方が同一のローカルエリアネットワークに接続されていると仮定することができる。図３５にその方法を示す。

【００１４】

図３５に示すように、あらかじめソース機器にシンク機器のネットワークアドレスＡを登録しておく（ステップＳ２１）。コンテンツを送受信する際に、ソース機器は自ネットワークアドレスとシンク機器のネットワークアドレスを比較し（ステップＳ２２，Ｓ２３）、一致すれば同一のローカルエリアネットワークに存在するものとして（ステップＳ２４）、コンテンツの送信を行う。その際、宛先がシンク機器のパケットのTTLフィールドを１にセットするように設定してもよい（ステップＳ２５）。一致しなければ、コンテンツの送受信処理を中止する（ステップＳ２６）。なお、この例ではソース機器が比較処理を行なっているが、逆にシンク機器が比較処理を行なってもよい。

【００１５】

【特許文献１】

特願２００２－１９１３５号

【特許文献２】

特開２００１－２８５２８４号公報

【００１６】

【発明が解決しようとする課題】

しかしながら、ソース機器やシンク機器に所定の設定を行うことで、ソース機器とシンク機器が物理的に同一のローカルエリアネットワークに接続されていなくても、仮想的に同一サブネットに存在するように見せることで、前述したネットワークアドレスの比較による同一のローカルエリアネットワークの限定を回避することができる。

【００１７】

VPNはその一例である。VPNとは、Virtual Private Networkの略で、インターネットに接続された遠隔地の計算機やルータ等の接続点とローカルエリアネットワークに接続された計算機が通信を行って仮想的にネットワークを構築することで、遠隔地の計算機がローカルネットワークに接続しているかのようにみせる技術の総称を指す。

【００１８】

VPNの例としては例えば、L2TPやPPTP、IPSecなどがある。ここでは、L2TPを例にとって説明する。なお、L2TP、PPTP及びIPSecについてはIETFにより標準化が進んでおり、http://www.ietf.orgにて取得可能に開示されている文書に説明が詳しい。

【００１９】

図３６はVPNを使ったネットワーク構成の一例を示す図である。図３６に示すように、ソース機器Ｂ１とシンク機器Ｃ９、およびVPNサーバ機器Ｄ６０が物理的なイーサネットセグメントＡ３に接続されており、同一のネットワークアドレスを持つことで、ローカルエリアネットワークＺ６１を構成している。またシンク機器A４とルータ機器E5は、同一のネットワークアドレスを持ち、ローカルエリアネットワークYを構成している。

【００２０】

VPNサーバ機器Ｄ６０はルーター機能を備え、インターネット６に接続されている。シンク機器Ａ４にはグローバルなアドレスが割り振られており、VPNクライアント機能を使ってインターネット６を経由してVPNサーバ機器Ｄ６０に接続して仮想ネットワークＸを構築している。この仮想ネットワークにシンク機器Ａ４が接続することになる。ここで重要なことは、シンク機器Ａ４はVPNで接続

することにより、仮想的にソース機器Ｂ１やシンク機器Ｃ９と同一のネットワークアドレスが割り振られていることである。

【００２１】

ここで、ソース機器Ｂ１からシンク機器Ａ４へコンテンツを送信する際に、前述したネットワークアドレスの比較による配布範囲の限定方法を適用してみる。

【００２２】

シンク機器Ａ４はソース機器Ｂ１と同一のネットワークアドレスを持つため、ネットワークアドレスは一致してしまう。シンク機器Ａ４がインターネット６に接続していればたとえ世界の裏側に配置されていたとしても、ソース機器Ｂ１はシンク機器Ａ４にコンテンツを送信することができてしまう。

【００２３】

またソース機器Ｂ１がIPパケットをTTL＝１にセットしてシンク機器Ａ４に送信したとしてもTTLの値は容易に改変可能であるため、例えば、VPNサーバ機器Ｄ６０とソース機器Ｂの間にTTLの値を改変するような機器を設置されてしまった場合、パケットはシンク機器Ａ４に到達可能となってしまう。

【００２４】

これは、ソース機器Ｂ１とシンク機器Ａ４のサブネットアドレスが同一だとしても、必ずしもこれらの機器は物理的に同一のローカルエリアネットワーク（この場合、イーサネットセグメント）に存在するとは限らない場合があることを意味する。

【００２５】

本発明は、このような点に鑑みてなされたものであり、その目的は、限られた受信装置だけにコンテンツを送信可能なコンテンツ送受信システム、コンテンツ送信装置、コンテンツ受信装置及びコンテンツ送受信方法を提供することにある。

【００２６】

【課題を解決するための手段】

上述した課題を解決するために、本発明は、送信装置と、この送信装置からコンテンツを受信する少なくとも１台の受信装置と、を備えたコンテンツ送受信シ

ステムにおいて、前記送信装置は、コンテンツ送信要求を行った前記受信装置との間で、認証・鍵交換処理を行う第１の認証・鍵交換処理手段と、前記受信装置の機器識別情報を送信するよう前記受信装置に対して機器識別情報要求を送信する機器識別情報送信要求手段と、前記受信装置から送信された前記機器識別情報を登録する機器識別情報登録手段と、前記受信装置のIP（Internet Protocol）アドレスに対応する前記機器識別情報を、前記受信装置が接続されているネットワークから検索する機器識別情報検索手段と、前記検索された機器識別情報と前記機器識別情報登録手段に登録されている機器識別情報とが一致するか否かを判定する比較判定手段と、前記比較判定手段による一致判定結果に応じて、コンテンツ送信要求を行った前記受信装置へのコンテンツの配布条件を変更する配布条件決定手段と、を有し、前記受信装置は、前記送信装置に対して前記コンテンツ送信要求を行うコンテンツ送信要求手段と、前記送信装置からの前記機器識別情報要求を受信すると、自装置の前記機器識別情報を前記送信装置に送信する機器識別情報送信手段と、を有する。

【００２７】

また、本発明は、少なくとも１台の受信装置に対してコンテンツを送信するコンテンツ送信装置において、コンテンツ送信要求を行った前記受信装置との間で、認証・鍵交換処理を行う認証・鍵交換処理手段と、前記受信装置の機器識別情報を送信するよう前記受信装置に対して機器識別情報要求を送信する機器識別情報送信要求手段と、前記受信装置から送信された前記機器識別情報を登録する機器識別情報登録手段と、前記受信装置のIPアドレスに対応する前記機器識別情報を、前記受信装置が接続されているネットワークから検索する機器識別情報検索手段と、前記検索された機器識別情報と、前記機器識別情報登録手段に登録されている機器識別情報と、が一致するか否かを判定する比較判定手段と、前記比較判定手段による一致判定結果に応じて、コンテンツ送信要求を行った前記受信装置へのコンテンツの配布条件を変更する配布条件決定手段と、を備える。

【００２８】

また、本発明は、送信装置からのコンテンツを受信するコンテンツ受信装置において、前記送信装置に対してコンテンツ送信要求を行うコンテンツ送信要求手

段と、コンテンツ送信要求先である前記送信装置との間で、認証・鍵交換処理を行う認証・鍵交換処理手段と、前記送信装置の機器識別情報を送信するよう前記送信装置に対して機器識別情報要求を送信する機器識別情報送信要求手段と、前記送信装置から送信された前記送信装置の機器識別情報を登録する機器識別情報登録手段と、前記送信装置のIPアドレスに対応する前記機器識別情報を、前記送信装置が接続されているネットワークから検索する機器識別情報検索手段と、前記検索された機器識別情報と、前記機器識別情報登録手段に登録されている機器識別情報と、が一致するか否かを判定する比較判定手段と、前記比較判定手段による一致判定結果に応じて、コンテンツ送信要求先である前記送信装置からのコンテンツ配布条件を決定する配布条件決定手段と、を備える。

【００２９】

また、送信装置と、この送信装置からコンテンツを受信する少なくとも１台の受信装置と、を備えたコンテンツ送受信システムにおいて、前記受信装置は、前記送信装置に対してコンテンツ送信要求を行うコンテンツ送信要求手段と、コンテンツ送信要求先である前記送信装置との間で、認証・鍵交換処理を行う第１の認証・鍵交換処理手段と、前記送信装置の機器識別情報を送信するよう前記送信装置に対して機器識別情報要求を送信する機器識別情報送信要求手段と、前記送信装置から送信された前記送信装置の機器識別情報を登録する機器識別情報登録手段と、前記送信装置のIPアドレスに対応する前記機器識別情報を、前記送信装置が接続されているネットワークから検索する機器識別情報検索手段と、前記検索された機器識別情報と、前記機器識別情報登録手段に登録されている機器識別情報と、が一致するか否かを判定する比較判定手段と、前記比較判定手段による一致判定結果に応じて、コンテンツ送信要求先である前記送信装置からのコンテンツ配布条件を決定する配布条件決定手段と、を有し、前記送信装置は、前記受信装置からの前記機器識別情報要求を受信すると、自装置の前記機器識別情報を前記受信装置に送信する機器識別情報送信手段と、コンテンツ送信要求を行った前記受信装置との間で、認証・鍵交換処理を行う第２の認証・鍵交換処理手段と、前記配布条件決定手段で決定された配布条件に従って、コンテンツの送信制御を行うコンテンツ送信制御手段と、を有する。

【００３０】

また、本発明は、送信装置からのコンテンツを受信可能なコンテンツ受信装置において、前記送信装置から自装置の機器識別情報検索要求があったか否かを判定する機器識別情報検索判定手段と、前記機器識別情報検索判定手段により前記機器識別情報検索要求がなかったと判定された場合には、前記送信装置からのコンテンツの受信を禁止するコンテンツ受信制御手段と、を備える。

【００３１】

また、本発明は、少なくとも１台の受信装置に対してコンテンツを送信可能なコンテンツ送信装置において、前記受信装置に対して、該受信装置の機器識別情報検索を事前通知する事前通知手段と、前記受信装置のIPアドレスに対応する前記機器識別情報を、前記受信装置が接続されているネットワークから検索する機器識別情報検索手段と、前記受信装置から送信された前記機器識別情報を登録する機器識別情報登録手段と、前記機器識別情報検索手段で検索された機器識別情報と、前記機器識別情報登録手段に登録された機器識別情報と、が一致するか否かを判定する比較判定手段と、前記受信装置から送信された、前記機器識別情報検索の事前通知に対する応答を受信したか否かを判定する要求応答受信判定手段と、前記比較判定手段及び前記要求応答受信判定手段による判定結果に基づいて、前記受信装置へのコンテンツの配布条件を決定する配布条件決定手段と、を備える。

【００３２】

また、本発明は、送信装置と、この送信装置からコンテンツを受信する少なくとも１台の受信装置と、を備えたコンテンツ送受信システムにおいて、前記送信装置は、前記受信装置に対して、該受信装置の機器識別情報検索を事前通知する事前通知手段と、前記受信装置のIPアドレスに対応する前記機器識別情報を、前記受信装置が接続されているネットワークから検索する機器識別情報検索手段と、前記受信装置から送信された前記機器識別情報を登録する機器識別情報登録手段と、前記機器識別情報検索手段で検索された機器識別情報と、前記機器識別情報登録手段に登録された機器識別情報と、が一致するか否かを判定する比較判定手段と、前記機器識別情報検索の事前通知に対する応答を受信したか否かを判定

する要求応答受信判定手段と、前記比較判定手段及び前記要求応答受信判定手段による判定結果に基づいて、前記受信装置へのコンテンツの配布条件を決定する配布条件決定手段と、を有し、前記受信装置は、前記送信装置からの前記機器識別情報要求を受信すると、自装置の前記機器識別情報及び機器識別情報の検索事前通知応答を前記送信装置に送信する自装置情報送信手段を有する。

【００３３】

また、本発明は、少なくとも１台の受信装置に対してコンテンツを送信可能なコンテンツ送信装置において、前記受信装置から自装置の機器識別情報検索要求があったか否かを判定する機器識別情報検索判定手段と、前記機器識別情報検索判定手段により前記機器識別情報検索要求がなかったと判定された場合には、前記受信装置へのコンテンツの送信を禁止するコンテンツ送信制御手段と、を備える。

【００３４】

また、本発明は、送信装置からのコンテンツを受信するコンテンツ受信装置において、前記送信装置に対して、該送信装置の機器識別情報検索を事前通知する事前通知手段と、前記送信装置に対してコンテンツ送信要求を行うコンテンツ送信要求手段と、コンテンツ送信要求先である前記送信装置との間で、認証・鍵交換処理を行う認証・鍵交換処理手段と、前記送信装置の機器識別情報を送信するよう前記送信装置に対して機器識別情報要求を送信する機器識別情報送信要求手段と、前記送信装置から送信された前記送信装置の機器識別情報を登録する機器識別情報登録手段と、前記送信装置のIPアドレスに対応する前記機器識別情報を、前記送信装置が接続されているネットワークから検索する機器識別情報検索手段と、前記検索された機器識別情報と、前記機器識別情報登録手段に登録されている機器識別情報と、が一致するか否かを判定する比較判定手段と、前記比較判定手段による一致判定結果に応じて、コンテンツ送信要求先である前記送信装置からのコンテンツ配布条件を決定する配布条件決定手段と、を備える。

【００３５】

また、本発明は、送信装置と、この送信装置からコンテンツを受信する少なくとも１台の受信装置と、を備えたコンテンツ送受信システムにおいて、前記送信

装置は、前記受信装置から自装置の機器識別情報検索要求があったか否かを判定する機器識別情報検索判定手段と、前記機器識別情報検索判定手段により前記機器識別情報検索要求がなかったと判定された場合には、前記受信装置へのコンテンツの送信を禁止するコンテンツ送信制御手段と、を有し、前記受信装置は、前記送信装置に対して、該送信装置の機器識別情報検索を事前通知する事前通知手段と、前記送信装置に対してコンテンツ送信要求を行うコンテンツ送信要求手段と、コンテンツ送信要求先である前記送信装置との間で、認証・鍵交換処理を行う認証・鍵交換処理手段と、前記送信装置の機器識別情報を送信するよう前記送信装置に対して機器識別情報要求を送信する機器識別情報送信要求手段と、前記送信装置から送信された前記送信装置の機器識別情報を登録する機器識別情報登録手段と、前記送信装置のIPアドレスに対応する前記機器識別情報を、前記送信装置が接続されているネットワークから検索する機器識別情報検索手段と、前記検索された機器識別情報と、前記機器識別情報登録手段に登録されている機器識別情報と、が一致するか否かを判定する比較判定手段と、前記比較判定手段による一致判定結果に応じて、コンテンツ送信要求先である前記送信装置からのコンテンツ配布条件を決定する配布条件決定手段と、を有する。

【００３６】

【発明の実施の形態】

以下、本発明に係るコンテンツ送受信システムについて、図面を参照しながら具体的に説明する。以下では、物理的なネットワークの一例としてイーサネットを用い、上位プロトコルにIPを使うものとする。もちろん、その他のプロトコル、例えばローカルエリアネットワークがIEEE1394で構成されていて、上位レイヤーとしてIPをエミュレーションしたIP over 1394であってもよい。

【００３７】

図１は本発明に係るコンテンツ送受信システムの第１の実施形態の概略構成を示すブロック図である。図１のコンテンツ送受信システムは、イーサネットセグメントＡ１０に接続されるシンク機器Ｂ１１、シンク機器Ｃ１２、ソース機器Ｄ及びルータ機器Ｆ１３と、ルータ機器Ｆ１３にインターネット１４を介して接続されるソース機器Ａ１５とを有する。シンク機器Ｂ１１はＶＰＮサーバ機能を持

ち、ソース機器Ａ１５はＶＰＮクライアント機能を持つものとする。

【００３８】

シンク機器Ｂ１１，Ｃ１２はそれぞれ同一のイーサネットセグメントＡ１０に接続されており、同一のネットワークアドレスを持つことにより、ローカルエリアネットワークを構成している。

【００３９】

ここで、コンテンツの配布範囲を一定の範囲内（ここではイーサネットセグメントＡ１０）に限定する方法について説明する。すなわち、物理的なイーサネットセグメントＡ１０に接続されたシンク機器Ｂ１１，Ｃ１２には、ソース機器Ｄ（要注意：図面１を修正）からのコンテンツの送受信を許可するが、ＶＰＮ機能を用いて別のイーサネットセグメントに接続されたソース機器Ａ１５からはコンテンツを送受信しないようにする。

【００４０】

本実施形態では、仮にシンク機器とソース機器がＶＰＮによって仮想的なネットワークを構築し、同一のローカルエリアネットワークに接続しているかのような構成をとっていたとしても、物理的にイーサネットセグメントに接続されている場合と、仮想的に接続している場合とを区別する点に特徴がある。

【００４１】

なお、ここではコンテンツの送受信にあたり、機器の認証・鍵交換及びコンテンツ暗号化・復号化の仕組みとしてDTCPを一例として説明する。DTCPとはDigital Transmission Contents Protectionの略で、IEEE1394やUSBなどでデファクトスターンダートとなっている著作権保護方式である。著作権保護が必要なAVデータなどのコンテンツに対して、送信機器と受信機器との間で認証・鍵交換を行い、AVデータを暗号化して転送する仕組みが備わっている（例えばhttp://www.dtla.comにて取得可能に開示されている文書に説明が詳しい）。

【００４２】

図２はソース機器Ａ１５とソース機器Ｄ１６の内部構成の一例を示すブロック図である。図２に示すように、ソース機器Ａ１５及びＤ１６は、イーサネットの物理レイヤ処理を実行するネットワークインターフェース部２１と、データリン

クレイヤ処理を実行する通信処理部２２と、シンク機器のネットワークインターフェースのMACアドレス（以下、単にＭＡＣアドレスと示す）をMACアドレステーブル２３に記録するMACアドレス記録部２４と、シンク機器のIPアドレスからMACアドレスを検索するシンク機器MACアドレス検索処理部２５と、シンク機器MACアドレス検索処理部２５から取得したMACアドレスとMACアドレス記録部２４に記録されたものとが一致しているか否かの検査を行うMACアドレス比較処理部２６と、著作権保護のためにDTCP認証・鍵交換処理を行う認証・鍵交換処理部２７と、送受信するデータを暗号・復号化するDTCP暗号処理部２８と、シンク機器に送信するコンテンツデータやDTCP管理データをIPパケットに変換するパケット処理部２９と、VPNサーバとしてVPNクライアントからVPN接続要求を受け付け、VPN接続を行うVPNサーバ部４０と、コンテンツをパケット処理部２９に供給するコンテンツ供給部３０とを有する。ここではVPNのプロトコルの一例としてL2TPを用いるものとする。L2TPとは、レイヤ２トンネリングプロトコル（Layer2 Tunneling Protocol）の略であり、VPNの実現手段として広く利用されている。L2TPについては、IETFにより標準化が進んでおり、http://www.ietf.orgにて取得可能に開示されている文書に説明が詳しい。

【００４３】

また、ここではソース機器Ａ１５とソース機器Ｄ１６を同一の構成として示してきたが、ソース機器Ｄ１６は必ずしもVPNサーバ部４０を備えている必要はない。なぜならば、ソース機器Ｄ１６とシンク機器Ｂ１１及びシンク機器Ｃ１２は同一のイーサネットセグメント上に接続されており、VPNを介して接続することが不要なためである。

【００４４】

なお、比較処理とは、コンテンツ送信先であるシンク機器のIPアドレスやデバイスＩＤに対応するMACアドレスがMACアドレステーブル２３に記録されており、かつ値が一致されているか否かの検索処理を行うことを示す。

【００４５】

図３はMACアドレステーブル２３の構造を示す図である。図３に示すように、各シンク機器に対応したIPアドレス、MACアドレス及びDTCPデバイスＩＤがレコ

ード毎に記録される。MACアドレス比較処理部２６は、MACアドレステーブル２３を使って、シンク機器から取得したIPアドレスやデバイスＩＤをキーとしてMACアドレスを検索する。

【００４６】

図４はシンク機器Ｂ１１，Ｃ１２の内部構成の一例を示すブロック図である。図４に示すように、シンク機器Ｂ１１，Ｃ１２はイーサネット物理レイヤ処理を実行するネットワークインターフェース部３１と、データリンクレイヤ処理を実行する通信処理部３２と、ネットワークインターフェース部３１に記憶されているMACアドレスを取得してソース機器に送信するMACアドレス送信部３３と、VPNクライアントとしてインターネットを経由してVPNサーバに接続するVPNクライアント部３４と、著作権保護のためのDTCP認証・鍵交換処理を行うDTCP認証・鍵交換処理部３５と、送受信するデータを暗号・復号化するDTCP暗号処理部３６と、ソース機器から受信したIPパケットをコンテンツデータやDTCP管理データに変換するパケット処理部３７と、復号化したコンテンツを表示装置などに出力したり蓄積するための処理を行うコンテンツ処理部３８とを有する。

【００４７】

ここではシンク機器Ｂ１１とＣ１２が同一の構成として示してきたが、ソース機器Ｄとシンク機器Ｃ１２が通信を行なう場合には、ＶＰＮで接続する必要はないため、シンク機器がＶＰＮクライアント部３４を備えていない構成もありうる。

【００４８】

なお、ここではソース機器A１５がVPNサーバ部４０を有し、シンク機器B１１がVPNクライアント部３４を有する構成を示したが、ソース機器A１５とシンク機器B１１がVPNにて通信を行うことが重要であり、VPNの機能を入れ替えた構成、すなわちソース機器A１５がVPNクライアント部３４を有し、シンク機器B１１がVPNサーバ部４０を有する構成となっていてもよい。

【００４９】

図５及び図６は本実施形態の通信システムの処理手順を示す図、図７はソース機器Ａ１５の処理手順を示す図である。以下、まず最初に、図６及び図７に沿っ

てソース機器Ｄからシンク機器Ｃ１２にコンテンツを送信する例を説明する。

【００５０】

まず、シンク機器Ｃ１２からソース機器Ｄ１６へコンテンツの送信要求がなされると（ステップＳ１）、DTCP認証・鍵交換処理が行なわれる（ステップＳ１２）。

【００５１】

なお、コンテンツの送信要求がなされた時点で、宛先のIPアドレスがシンク機器Ｃ１２に対して著作権保護に関する認証・鍵交換等の管理データ及びコンテンツを送信する際にはIPパケットのTTLフィールドを１に設定してもよい（ステップＳ２，Ｓ１１）。また、従来の技術で述べたように、シンク機器とソース機器のネットワークアドレスが一致するか否かの比較処理を行なってもよい。この場合、シンク機器Ｃ１２とソース機器Ｄ１６のネットワークアドレスが異なる場合には、所定のエラー処理を行い、通信を中止すればよい。これらの処理は、DTCP認証・鍵交換処理を行う前に行ってもよいし、同処理の途中あるいは後に行ってもよい。

【００５２】

DTCP認証・鍵交換処理が成功すると（ステップＳ３）、ソース機器Ｄ１６はシンク機器Ｃ１２に対してMACアドレスの送信を要求するコマンドを送信する（ステップＳ４）。このコマンドは独立したコマンドでもよいし、DTCPで定義されるコマンド群に「MACアドレス要求コマンド」を追加したものでもよい。シンク機器Ｃ１２はMACアドレス要求コマンドを受信すると、アドレス送信部３３を介してソース機器Ｄ１６にMACアドレスを送信する（ステップＳ５）。

【００５３】

この時、通信経路上でMACアドレスが改ざんされていないことを示すために署名をつけてもよい。この署名の方法は、例えばISO/IEC14888のような、よく知られた方法を用いればよい。

【００５４】

ソース機器Ｄ１６はシンク機器Ｃ１２のMACアドレスを取得すると（ステップＳ１３）、MACアドレステーブル２３に登録する（ステップＳ６，Ｓ１４）。こ

のとき、MACアドレスとシンク機器Ｃ１２のIPアドレスやDTCPデバイスIDを組として記録してもよい。

【００５５】

以上は、MACアドレスをシンク機器Ｃ１２からネットワークを経由して受信することで、シンク機器Ｃ１２のMACアドレステーブル２３に登録する方法である。登録方法については、この他にも種々の方法が考えられる。例えば、（１）あらかじめ利用者がソース機器Ｄ１６にシンク機器Ｃ１２のMACアドレスをボタン等のインターフェースを用いて入力する方法、（２）シンク機器Ｃ１２のＭＡＣドレスが記録されたカード等を用いてソース機器ＤのＭＡＣアドレステーブルに記録する方法などが考えられる。

【００５６】

次に、ソース機器Ｄ１６はIPアドレスからMACアドレスの問い合わせを行うパケットをイーサネットセグメントＡ１０に送信する。この仕組みはよく知られた方法、例えばRFC826にて規定されたARP（アドレス解決プロトコル）を用いればよい。物理的に同一セグメントに接続されていれば、応答としてIPアドレスを持つホストは自機器に付与されたMACアドレスを返す（ステップＳ８，Ｓ１５）。例えば、ソース機器Ｄ１６がIPアドレス192.168.1.5に対してARPのリクエストを送信したとすると、IPアドレスが192.168.1.5に設定されたシンク機器Ｃ１２はその応答として、ソース機器Ｄ１６に自身のMACアドレス「CC:CC:CC」を返すことになる。

【００５７】

次に、ソース機器Ｄ１６は、MACアドレス要求コマンドの結果として取得したシンク機器Ｃ１２のMACアドレスとARPによって取得したMACアドレスが一致するかの比較処理を行う（ステップＳ９，Ｓ１６）。もし二つの値が一致していれば処理を継続する（ステップＳ１７，Ｓ１８）。

【００５８】

上述したステップＳ７にて、MACアドレステーブル２３から通信相手のシンク機器のMACアドレスを検索する際に、検索のキーとしてIPアドレスだけでなく、デバイスIDをキーとしてMACアドレスを検索してもよい。

【００５９】

上述したステップＳ１６の比較処理において、MACアドレスが一致していなければ所定のエラー処理を行い、通信を中止する（ステップＳ１０，Ｓ１９）。また、ARPによってシンク機器Ｃ１２のMACアドレスが取得できない場合も所定のエラー処理を行い、通信を中止する。この例では、事前にMACアドレスリストに登録した値とARPによって取得した値は同一であるため、コンテンツ送信処理が行なわれる。

【００６０】

次に、ソース機器Ａ１５からシンク機器Ｂ１１にコンテンツを送信する例を図５に示す。ソース機器Ａ１５はＶＰＮにてシンク機器Ｂ１１に接続されており、通信可能な状態にある。ソース機器Ａ１５がシンク機器Ｂ１６にＭＡＣアドレスを要求し、ＩＰよりも上位のプロトコルでシンク機器Ｂ１１のＭＡＣアドレスを取得し、記録する処理（ステップＳ６）まではソース機器Ｄからシンク機器Ｃ１２と同様の方法で行なえばよい。ソース機器Ａ１５はシンク機器Ｂ１１のIPアドレスからMACアドレスの問い合わせを行うパケット（例えばＡＲＰパケット）を、ソース機器Ａ１５が接続されている不図示のイーサネットセグメントに送信する。この場合、シンク機器Ｂ１１は不図示のイーサネットセグメントに接続されていないため、シンク機器Ｂ１１が応答として自身のMACアドレス「CC:CC:CC」を返すことはない。このため、ソース機器Ａ１５がシンク機器Ｂ１１のＭＡＣアドレスを取得することはなく、ＭＡＣアドレス比較処理は失敗する。これにより、ソース機器はエラー処理を行い、シンク機器Ｂ１１に対してコンテンツを送信することなく通信を終了する。

【００６１】

なお、MACアドレス不一致の際のエラー処理や、シンク機器とのコネクション切断時に、シンク機器に関するレコードを記憶しておいてもよいし、消去してもよい。例えばシンク機器のIPアドレスがDHCPによって割り振られた場合、次回接続時にIPアドレスは変化する可能性があるため、消去した方が、テーブルに割り当てる記憶容量を節約でき、機器の構成を簡単にすることができる。

【００６２】

さて、これまでDTCP認証・鍵交換処理によって、認証された場合にのみMACアドレスの確認処理を行う例を示した。この他にもMACアドレスの確認を行うには、（１）シンク機器がコンテンツ要求をソース機器に送信する際にDTCPのコンテンツ要求コマンドとルーター共にMACアドレスを付加して送信する方法、（２）DTCP認証・鍵交換処理に先立ち、MACアドレスの確認処理を行う方法などがある。

【００６３】

ここで重要なことは、シンク機器がソース機器にイーサネットよりも上位のプロトコルでMACアドレスを送信する機能を持ち、イーサネット上でIPアドレスからMACアドレスを検索する処理で得たMACアドレスとを比較することで、ソース機器とシンク機器が同一サブネットであっても、イーサネットセグメントに物理的に接続されているのか、そうでないかを判別することができる点である。

【００６４】

仮に、ソース機器Ａ１５のMACアドレス要求に対する応答として、ソース機器Ａ１５と物理的に同一のイーサネットセグメントに接続されている不図示のルーター機器が、MACアドレスを偽り、シンク機器Ｂ１１のMACアドレスと同一のMACアドレスを送信したとしても、ソース機器Ａ１５はその偽ったMACアドレスにイーサネットパケットを送信するため、シンク機器Ｂ１１がこのパケットを受信することができず、コンテンツの配布範囲を限定する目的は達成できる。

【００６５】

次に、図８に示すように、ソース機器とシンク機器との間にＶＰＮサーバ機器５３が接続されている場合のコンテンツ送受信について説明する。図８のコンテンツ送受信システムは、同一のイーサネットセグメントＡ５０に接続されるソース機器Ｂ５１、シンク機器Ｃ５２、VPNサーバ機器Ｆ５３及びルータ機器Ｄ５４と、インターネット５５を介してVPNサーバ機器Ｆ５３に接続されるシンク機器Ａ５６と、イーサネットセグメントＢ５７に接続されるシンク機器Ｅ５８とを備えている。

【００６６】

ソース機器Ｂ５１、シンク機器Ｃ５２、VPNサーバ機器Ｆ５３及びルータ機器Ｄ５４はそれぞれ同一のネットワークアドレスを持つことにより、ローカルネッ

トワークを構成している。

【００６７】

シンク機器Ａ５６には、グローバルなIPアドレスが割り振られており、VPNクライアント機能を使ってインターネットを経由してVPNサーバ機器Ｄに接続可能な状態にある。

【００６８】

図８のコンテンツ送受信システムにおいて、ソース機器Ｂ５１からVPNサーバ機器Ｆ５３を経由して、仮想的に接続しているシンク機器Ａ５６にコンテンツを送信する場合を考える。

【００６９】

まず、ソース機器Ｂ５１がシンク機器Ａ５６からMACアドレスを受信し、登録するまでは上記手続きと同じでよい。その後、ソース機器Ｂ５１はシンク機器Ａ５６のIPアドレスからMACアドレスの問い合わせを行うパケットをイーサネットセグメントＡ５０に送信する。

【００７０】

シンク機器Ａ５６は物理的なイーサネットセグメントＡ５０に接続されていないため、VPNサーバ機器Ｆ５３が自身のMACアドレスを代理でシンク機器Ａ５６のMACアドレスとして応答を返す。ソース機器Ｂ５１はこれら二つのMACアドレスの比較処理を行うが、シンク機器Ｅ５８とVPNサーバ機器Ｆ５３のMACアドレスは異なるため、値は一致しない。このため、コンテンツ送信処理は中止される。

【００７１】

次に、ソース機器Ｂ４３からシンク機器Ｅ４７にコンテンツを送信する場合を考える。ソース機器Ｂ４３はシンク機器Ｅ４７にＭＡＣアドレスを要求し、ＩＰよりも上位のプロトコルでシンク機器Ｅ４７のＭＡＣアドレスを取得する。しかしこの構成では、ソース機器Ｂ４３の接続するイーサネットセグメントＡ５０と、シンク機器Ｅの接続するイーサネットセグメントＢ５７は異なる。従って、ソース機器Ｂ４３は、シンク機器Ｅ４７のＩＰアドレスからＭＡＣアドレスの問い合わせ処理を行なうパケットを送信したとしても、当該パケットはルータ機器によってシンク機器Ｅに転送されることはなく、ソース機器Ｂ４３はシンク機器Ｅ

４７からＭＡＣアドレスを受信することはない。これにより、ソース機器Ｂ５１で行なうＭＡＣアドレスの比較処理は失敗し、コンテンツの送信処理が中止される。

【００７２】

以上の処理により、図８のソース機器Ｂ５１は、同一イーサネットセグメントＡ５０に接続されるシンク機器Ｃ５２にはコンテンツの送受信を許可するが、VPNサーバ機器Ｆ５３を介して接続されるシンク機器Ａ５６や、ルータ機器Ｄ５４を介して異なるイーサネットセグメントＢ５７に所属するシンク機器Ｅ５８に対するコンテンツの送受信を確実に禁止できる。

【００７３】

このように、本実施形態によれば、例えば図８のような構成のコンテンツ送受信システムにおいて、ソース機器Ｂ５１は同一イーサネットセグメントＡ５０に接続されているシンク機器Ｃ５２のみにコンテンツの送受信を許可するため、例えばVPNサーバ機器Ｆ５３を介して接続されるシンク機器等へのコンテンツの送受信を確実に禁止できる。これにより、コンテンツの不正な送受信を防止できる。

【００７４】

以上は、シンク機器Ａ５６にＶＰＮクライアントが備わっており、ＶＰＮサーバＦ５３を経由してイーサネットセグメントＡに接続する構成について説明をしてきたが、本実施形態は、ソース機器にＶＰＮクライアントが備わっている構成になっていてもよい。

【００７５】

図９はソース機器とシンク機器の接続関係を第１の実施形態とは逆にした場合の概略構成を示すブロック図である。図９のコンテンツ送受信システムは、図８と異なり、VPNクライアント機能を持ち、インターネット１５を経由してVPNサーバ機器Ｆ１３に接続されるソース機器Ａ４１と、イーサネットセグメントＡ４２に接続されるシンク機器Ｂ４３、シンク機器Ｃ４４及びルータ機器Ｄ４５と、ルータ機器Ｄ４５にイーサネットセグメントＢ４６を介して接続されるシンク機器Ｅ４７とを有する。

【００７６】

すなわち、VPNサーバ機器Ｆ１３に接続されるシンク機器Ｂ４３及びシンク機器Ｃ４４は、ＶＰＮサーバＦ１３を経由してソース機器Ａ４１と通信可能な位置に存在する。しかし、ソース機器Ａ４１とシンク機器Ｂ４３、Ｃ４４は異なるローカルエリアネットワークに接続されているため、著作権を保護すべきコンテンツの送受信は許可されるべきではないものとする。

【００７７】

ここで、ソース機器Ａ４１がシンク機器Ｂ４３に対してＭＡＣアドレスを要求し、ＩＰよりも上位のプロトコルでシンク機器Ｂ４３のＭＡＣアドレスを取得する。ソース機器Ａ４１はシンク機器Ｂ４３のIPアドレスからMACアドレスの問い合わせを行うパケット（例えばＡＲＰパケット）を、ソース機器Ａ４１が接続されている不図示のイーサネットセグメントに送信する。この場合、シンク機器Ｂ４３は不図示のイーサネットセグメントに接続されていないため、シンク機器Ｂ４３が応答として自身のMACアドレス「BB:BB:BB」を返すことはない。このため、ソース機器Ａ４１がシンク機器Ｂ４３のＭＡＣアドレスを取得することはなく、ＭＡＣアドレス比較処理は失敗する。これにより、ソース機器はエラー処理を行い、シンク機器Ｂ４３に対してコンテンツを送信することなく通信を終了する。これにより、ＶＰＮを介したコンテンツの送受信を防ぐことができ、ソース機器Ａ４１がコンテンツの配布範囲をソース機器Ａ４１のローカルエリアネットワーク内に制限することができる。

【００７８】

（第２の実施形態）

第２の実施形態はシンク機器とソース機器の間にVPNサーバ機器とVPNクライアント機器を設置し、VPN機器が二つのネットワークをトンネリングする構成にしたものである。

【００７９】

図１０はシンク機器Ａ４８とソース機器Ｂ４３の間にVPNサーバ機器Ｆ１３とVPNクライアント機器Ｇ４９を設置し、VPNサーバ機器Ｆ１３とVPNクライアント機器Ｇ４９が二つのネットワークをトンネリングするコンテンツ送受信システムの

ブロック構成を示している。図１０で示したコンテンツ送受信システムの形態におけるソース機器の内部構成は図１１のようなブロック図で表され、シンク機器の内部構成は図１２のようなブロック図で表される。

【００８０】

図１や図８と異なり、図１０のコンテンツ送受信システムは、シンク機器Ａ４８とソース機器Ｂ４３との間にVPNサーバ機器Ｆ１３とVPNクライアント機器Ｇ４９があり、それぞれのネットワークを接続している。しかしながら、ソース機器Ｂ４３の所属するイーサネットセグメントＡ４２とシンク機器Ａ４８の所属するイーサネットセグメントＢ４６は互いに異なるため、ソース機器Ｂ４３のMACアドレス検索要求からシンク機器Ａ４８のMACアドレスを取得することはできず、比較処理は失敗する。これにより、シンク機器Ａ４８がソース機器Ｂ４３の所属するイーサネットセグメントＡ４２に存在しないことを確認できる。

【００８１】

このように、第２の実施形態においても、MACアドレスを比較して、比較結果が一致した場合のみコンテンツの送信を許可することにより、異なるイーサネットセグメントに接続されたシンク機器へのコンテンツ送信を確実に禁止できる。

【００８２】

上述した各実施形態において、ソース機器からの要求に従ってシンク機器が自己のMACアドレスを送信する際、MACアドレスとともに電子署名を添付して送信してもよい。ソース機器は、シンク機器からのMACアドレスに電子署名が添付されていた場合は、MACアドレスが改ざんされているか否かの検証処理を行い、改ざんされていない場合にのみMACアドレスをMACアドレステーブルに記録する。これにより、MACアドレスの偽造を確実に防止でき、セキュリティ性能の向上が図れる。

【００８３】

上述した各実施形態では、ソース機器の内部でMACアドレスの比較を行う例を説明したが、コンテンツの受け取り側であるシンク機器の内部でMACアドレスの比較を行ってもよい。例えば、図１に示した構成でのソース機器Ａ１５に対応するシンク機器とソース機器の役割を入れ替えた構成にした場合のソース機器の内

部構成は図１３のようなブロック図で表され、シンク機器Ｂ１１の内部構成は図１４のようなブロック図で表される。

【００８４】

この場合、ソース機器が自機器のＭＡＣアドレスをシンク機器に送信し、シンク機器内でのMACアドレスの比較結果が一致した場合のみ、ソース機器からコンテンツの受信を受付を行ったり、場合によっては受信拒否のメッセージをシンク機器に対して送信したりすることで、コンテンツの送信先を限定することができる。

【００８５】

図１５はVPN機器の接続形態の種類を示す図である。VPN機器は、それ自身でルーティングを行うため、TTLの減算を行う。すなわち、図１５に示すようにVPN機器を介してシンク機器とソース機器が通信を行うには、IPヘッダのTTLフィールドを適切な値以上に設定しなければならない。

【００８６】

例えば、図１５の環境Ａの構成では、VPN機器がルーティングを行うため、各VPN機器でTTLフィールドの減算を行う。したがって、シンク機器Ａ－Ａとソース機器Ａ－Ｂが通信を行うには、TTLの値を3以上に設定しなければならない。同様に、環境Ｂの構成でも、シンク機器Ｂ－Ａとソース機器Ｂ－Ｂが通信を行うには、TTLの値を3以上に設定しなければならない。

【００８７】

従って、TTLの値を１に設定すれば、環境Ａや環境ＢではVPN装置を介したコンテンツの配布を制限することができる。ここで注意すべきは、TTLフィールドが容易に改変可能だということである。例えば悪意ある利用者がTTLフィールドを一定の値に増加させるTTL改変装置をソース機器とVPN機器の間に設置したとすると、ソース機器、及びシンク機器が想定する配布範囲を超えてコンテンツを送受信することが可能となってしまう。

【００８８】

しかしながら、上述した手法を用いれば、例えTTL改変装置を設置されたとしても、ソース機器とシンク機器は物理的な同一セグメントに所属していないため

、依然としてARPによって互いのMACアドレスを知ることができず、TTL改変装置の影響を受けることはない。

【００８９】

すなわち、本実施形態によれば、環境Ａ、Ｂ、Ｃに係らず統一的にVPNの存在を検出することができ、コンテンツの配布範囲を限定することができる。

【００９０】

（第３の実施形態）

上述した第１及び第２の実施形態において、ソース機器と物理的に同一のイーサネットセグメントに接続されたルータ機器やVPN機器にシンク機器と同一のMACアドレスを設定してしまうと、ソース機器とシンク機器が物理的に同一のイーサネットセグメントに接続されているか否かを正確に判断できなくなるおそれがある。

【００９１】

そこで、以下に説明する第３の実施形態は、このような不具合を解決することを特徴とする。

【００９２】

図１６は本発明に係るコンテンツ送受信システムの第３の実施形態の概略構成を示すブロック図である。図１６のVPNサーバ機器Ｆ５３は、図８と異なり、シンク機器Aと同一のMACアドレスの値AA:AA:AAを持つ。

【００９３】

原則として、MACアドレスは、各製造ベンダにより、物理的なネットワークインターフェースごとに異なる値が付与されることになっている。しかし、この原則から外れてMACアドレスが一致してしまった場合や、悪意のある利用者がMACアドレス比較のチェック処理を回避するために、VPNサーバ、もしくはルーター機器にシンク機器と同じ値のMACアドレスをつけたとする。

【００９４】

この場合、ソース機器Ｂ５１がイーサネット上でIPアドレスからMACアドレスを検索する処理(例えばARP)で得るMACアドレスの値はVPNサーバ機器のMACアドレスであるAA:AA:AAとなる。その結果、上位のプロトコルによって取得したシンク

機器AのMACアドレスAA:AA:AAと、IPアドレスからMACアドレスを検索する処理で得るMACアドレスの値は一致してしまうため、ソース機器とシンク機器が同一のイーサネットセグメントに物理的に接続されているのか、そうでないのかを判別することができない。

【００９５】

第３の実施形態では、仮にソース機器に物理的に同一のイーサネットセグメントに接続されたVPN機器またはルーター機器が、シンク機器と同一のMACアドレスを保持していたとしても、ソース機器とシンク機器間でアドレス解決要求を確実に行ったかどうかを確認することで、ソース機器とシンク機器が物理的に同一のセグメントにいるのか、そうでないのかを確認できるようにしている。

【００９６】

図１７は第３の実施形態におけるソース機器Ｂ５１の内部構成を示すブロック図である。図２との相違点は、シンク機器にIPアドレスからMACアドレスを検索するためのメッセージを送信する前に、「これからMACアドレス検索要求を送る」ことを明示的に通知するメッセージ（以下、このメッセージをMACアドレス検索事前通知と呼ぶ）を送信したり、検索事前通知応答がシンク機器から送信されたかどうか確認する処理を行うMACアドレス検索事前通知処理部６２を有する点である。

【００９７】

図１８は第３の実施形態におけるシンク機器Ａ５６の内部構成を示すブロック図である。図４と異なる点は、ソース機器から送信されたMACアドレス検索事前通知を受信して所定の処理を行うMACアドレス検索事前通知受信処理部６３を有する点である。

【００９８】

図１９は第３の実施形態の処理手順を示すシーケンス図であり、ソース機器とシンク機器が物理的に同一のセグメントに存在する場合（例えば、図８に示すソース機器Ｂ５１とシンクＣ５２が通信を行う場合）の処理手順を示している。

【００９９】

ここでは、説明を簡略化するために、図５に示すようなDTCP認証・鍵交換処理

（ステップＳ３）、MACアドレス要求（ステップＳ４）及びMACアドレス送信（ステップＳ５）が行われており、DTCP認証・鍵交換が成功し、ソース機器がシンク機器のMACアドレスを取得しているものとする。

【０１００】

まず、ソース機器はIPアドレスからMACアドレスを検索する要求メッセージとMACアドレス検索事前通知とをシンク機器に送信する（ステップＳ３１～Ｓ３３）。MACアドレス検索事前通知はイーサネットよりも上位のプロトコル（例えばIPパケット）にて送信すればよい。なお、これらのメッセージは同時に送信してもよいし、別々に送信してもよい。

【０１０１】

シンク機器は、MACアドレス検索の応答として、自機器のMACアドレスをソース機器に送信する（ステップＳ３４）。また、シンク機器は、ソース機器から送信されたMACアドレス検索を受信したことを記録しておく。

【０１０２】

ソース機器はMACアドレス検索要求によって受信したMACアドレスと事前に取得したMACアドレスとの比較処理を行う（ステップＳ３５）。ここではMACアドレスが一致するため、比較処理は成功し、ソース機器はコンテンツをシンク機器に送信する（ステップＳ３６）。

【０１０３】

一方、シンク機器はMACアドレス検索要求を受信しているか否かの確認処理を行う（ステップＳ３７）。ここでは、もしもソース機器からMACアドレスを検索する要求メッセージを受信していれば、処理を継続する（ステップＳ３８）。MACアドレス検索要求を受信していなければ、処理を中止するものとする。この場合、シンク機器はステップＳ３３でMACアドレス検索要求を受信しているため、このチェック処理は成功し、コンテンツの受信が開始される。

【０１０４】

図２０はソース機器とシンク機器が物理的に同一のセグメントに存在しない場合（例えば図８に示すソース機器Ｂ５１とシンク機器Ａ５６が通信する場合）における第３の実施形態の処理手順を示すシーケンス図である。

【０１０５】

図１９の場合と同様に、まず、ソース機器はIPアドレスからMACアドレスを検索する要求メッセージとMACアドレス検索事前通知とをシンク機器に送信する（ステップＳ４１，Ｓ４２）。

【０１０６】

MACアドレス検索事前通知は、イーサネットよりも上位のプロトコルでシンク機器に送信されるため、途中にVPNサーバが存在しても、シンク機器はMACアドレス検索事前通知を受信する。

【０１０７】

ところが、IPアドレスからのMACアドレス検索要求に関しては、シンク機器は物理的に同一のイーサネットセグメントに接続しておらず、VPNサーバ機器が代理で応答してしまうため（ステップＳ４３）、シンク機器はこの検索要求を受信できない。

【０１０８】

ここで、仮にVPNサーバ機器のMACアドレスとシンク機器のMACアドレスが一致していた場合、ソース機器でのMACアドレス比較処理は成功してしまうため（ステップＳ４４）、ソース機器はシンク機器が物理的に同一のイーサネットセグメントに存在しないにも関わらず、コンテンツを送信してしまう（ステップＳ４５）。

【０１０９】

一方、シンク機器は、MACアドレスの検索要求メッセージを受信しているか否かを確認し（ステップＳ４６）、この要求メッセージを受信していないことがわかると、コンテンツの受信を中止する（ステップＳ４７）。そして、ソース機器に対してコンテンツの送信中止依頼メッセージを送信し（ステップＳ４８）、ソース機器は当該メッセージを受信するとシンク機器に対してコンテンツの送信を中止するようにしてもよい（ステップＳ４９）。

【０１１０】

このように、第３の実施形態では、シンク機器がMACアドレスを検索する要求メッセージを受信したか否かによって、仮にソース機器とシンク機器の間に、I

ＰアドレスからＭＡＣアドレスを検索する要求に対してＭＡＣアドレスを偽って応答する機器が存在していたとしても、ソース機器とシンク機器が物理的に同一のセグメントにいるのか、そうでないのかを確認することができる。

【０１１１】

なお、第３の実施形態では、シンク機器がソース機器からMACアドレス検索を受信できれば、ソース機器からMACアドレス検索事前通知をシンク機器に送信する必要は必ずしもない。ただし、MACアドレスを検索する要求メッセージがソース機器から送られたものであることを確認するためには、MACアドレス検索事前通知にソース機器のMACアドレスやIPアドレス、もしくはその両方を含めてシンク機器に送信すればよい。これにより、MACアドレスの検索要求をシンク機器が受信した際に、それがソース機器からなされたものであるか、そうでないかを区別することが出来る。

【０１１２】

また、シンク機器は、MACアドレス検索事前通知を受信することにより、MACアドレス検索を監視する必要性を把握できるため、MACアドレス検索事前通知を受信するまではMACアドレス検索を監視する必要がなくなり、平常時におけるシンク機器の処理負荷を軽減することができる。

【０１１３】

（第４の実施形態）

第４の実施形態は、シンク機器がソース機器と同一のセグメントに存在するか否かを第３の実施形態とは異なる処理手順で確認するものである。

【０１１４】

図２１はソース機器の第４の実施形態の内部構成を示すブロック図である。図２１のソース機器は、図１７のソース機器の構成に加えて、シンク機器からのMACアドレス検索事前通知応答が受信されたか否かを判断するMACアドレス検索事前通知応答受信処理部６４を有する。

【０１１５】

図２２はシンク機器の第４の実施形態の内部構成を示すブロック図である。図２２のシンク機器は、図１８のシンク機器の構成に加えて、ソース機器からのMA

Cアドレス検索事前通知に対する応答であるMACアドレス検索事前通知応答をソース機器に送信する制御を行うMACアドレス検索事前通知応答処理部６５を有する。

【０１１６】

図２３は第４の実施形態の処理手順を示すシーケンス図であり、ソース機器とシンク機器が物理的に同一のセグメントに存在する場合（例えば、図８に示すソース機器Ｂ５１とシンクＣ５２が通信を行う場合）の処理手順を示している。なお、ここでも説明を簡単にするために、図１９、図２０と同様に、DTCP認証・鍵交換は成功し、ソース機器が上位のプロトコルでシンク機器のMACアドレスを取得しているものとする。

【０１１７】

まず、ソース機器はIPアドレスからMACアドレスを検索する要求メッセージとMACアドレス検索事前通知とをシンク機器に送信する（ステップＳ５１，Ｓ５２）。なお、これらのメッセージは同時に送信してもよいし、別々に送信してもよい。

【０１１８】

シンク機器は、MACアドレス検索要求の応答として、自機器のMACアドレスと検索事前通知応答とを含むメッセージをソース機器に送信する（ステップＳ５３）。この検索事前通知応答はイーサネットよりも上位のプロトコル（例えばIPパケット）にて送信すればよい。また、検索事前通知応答のメッセージに、検索要求元、または検索結果送信先のMACアドレスを含めて送信してもよい。

【０１１９】

ソース機器は、IPアドレスからのMACアドレス検索の応答として、MACアドレスと検索事前通知応答のメッセージを受信する（ステップＳ５４）。なお、このメッセージメッセージが改変されていないことを示すために、シンク機器が署名をつけたり、タイムスタンプをつけて送信し、ソース機器でこの署名を確認する処理を付け加えてもよい。

【０１２０】

ソース機器はMACアドレス検索要求によって受信したMACアドレスとMACアドレ

ス要求によって事前に取得したMACアドレスとの比較処理を行う（ステップＳ５５）。ここではMACアドレスが一致するため、比較処理は成功する。

【０１２１】

また、ソース機器は、検索事前通知応答を受信しているか否かの確認を行う（ステップＳ５６）。この確認処理は、もしもシンク機器から検索事前通知応答メッセージを受信していれば処理を継続し、受信していなければ処理を中止するものとする。ここでは、ステップＳ５４でMACアドレス検索事前通知応答を受信しているため、このチェック処理は成功し、コンテンツの送信が開始される（ステップＳ５７）。

【０１２２】

なお、検索事前通知応答メッセージにタイムスタンプが含まれている場合、タイムスタンプT1の値がソース機器がMACアドレス検索事前通知を送った時刻T0よりも後で、なおかつMACアドレスを受信した時刻T2よりも前であることを確認してもよい。

【０１２３】

図２４はソース機器とシンク機器が物理的に同一のセグメントに存在しない場合（例えば、図８に示すソース機器Ｂ５１とシンク機器Ａ５６が通信する場合）における第４の実施形態の処理手順を示すシーケンス図である。

【０１２４】

まず、ソース機器はIPアドレスからのMACアドレス検索とMACアドレス検索事前通知とをシンク機器に送信する（ステップＳ６１，Ｓ６２）。MACアドレス検索事前通知はイーサネットよりも上位のプロトコルで送信されるため、シンク機器によって受信される。ところが、IPアドレスからのMACアドレス検索要求に関しては、シンク機器は物理的に同一のイーサネットセグメントに接続しておらず、VPNサーバ機器が代理で応答してしまうため（ステップＳ６３）、シンク機器は受信できない。このため、シンク機器はIPアドレスからのMACアドレス検索の応答とMACアドレス検索事前通知応答とをソース機器に送信することはない。

【０１２５】

一方、ソース機器は、VPNサーバ機器からMACアドレスを受信する。ここで、仮

にVPNサーバ機器のMACアドレスとシンク機器のMACアドレスが一致していた場合、ソース機器でMACアドレス比較処理は成功してしまう（ステップＳ６４）。しかし、検索事前通知応答は受信していないため、この確認処理は失敗し（ステップＳ６５）、ソース機器はコンテンツの送信を中止する（ステップＳ６６）。

【０１２６】

ここで注意すべきは、IPアドレスからMACアドレスを検索する要求メッセージはソース機器に限らず、一般のルーター機器などが送信することである。このため、シンク機器はどの要求メッセージに応答するMACアドレス検索事前通知応答をソース機器に送ればよいのかわからない。そのため、MACアドレス検索事前通知にて、ソース機器のIPアドレス、MACアドレスまたはその両方を送信することで、シンク機器は特定のIPアドレスもしくはMACアドレスから送信される要求メッセージに対してMACアドレス検索事前通知応答を送ればよいのか区別することができる。

【０１２７】

このように、第４の実施形態では、ソース機器からシンク機器に上位レイヤによりMACアドレス検索事前通知を送信するため、たとえソース機器とシンク機器の間に、シンク機器と同じＭＡＣアドレスを持つルータ機器やＶＰＮ機器が存在していたとしても、この通知に対する応答があったか否かで、シンク機器がソース機器と同一のセグメントに接続されているか否かを正確に判断でき、コンテンツの著作権保護が図れる。

【０１２８】

また、このMACアドレス検索事前通知とその応答は、コンテンツの著作権保護を目的したものであり、この判断を誤らせるために、MACアドレス検索事前通知に対する応答を偽って送信するような機器を設置することは、コンテンツの著作権保護を迂回するために意図的に設置したとみなすことができる。

【０１２９】

なお、以上では、MACアドレス検索事前通知とMACアドレス検索事前通知応答は、イーサネットよりも上位のレイヤーを用いることを前提としてきたが、DTCPで定義されるコマンド群の一つとして定義してもよい。この場合、DTCP認証・鍵交

換の処理の一部として、MACアドレス検索事前通知、及びMACアドレス検索事前通知応答を実現することができるため、機器の構成を簡略化することができる。

【０１３０】

（第５の実施形態）

上述した第５の実施形態では、ソース機器がMACアドレス検索事前通知をシンク機器に送信し、シンク機器がMACアドレス検索事前通知応答をソース機器に送信する構成について説明したが、以下に説明する第５の実施形態は、シンク機器がMACアドレス検索事前通知をソース機器に送信し、ソース機器がMACアドレス検索事前通知応答をシンク機器に送信するものである。

【０１３１】

図２５はソース機器の第５の実施形態の内部構成を示すブロック図である。図２５のソース機器は、図１７のソース機器からMACアドレス記録部２４、MACアドレス検索処理部２５及びMACアドレス比較処理部２６を省略し、その代わりに図１８のシンク機器と同様のMACアドレス検索事前通知受信処理部６３、VPNクライアント部及びMACアドレス送信部を追加した構成になっている。

【０１３２】

図２６はシンク機器の第５の実施形態の内部構成を示すブロック図である。図２６のシンク機器は、図１８のシンク機器からMACアドレス検索事前通知受信処理部６３、VPNクライアント部及びMACアドレス送信部を省略し、その代わりに図１７のソース機器と同様のMACアドレス記録部２４、MACアドレス検索処理部２５、MACアドレス比較処理部２６及びMACアドレス検索事前通知処理部６２を追加した構成になっている。

【０１３３】

図２７はソース機器とシンク機器が物理的に同一のセグメントに存在する場合における第５の実施形態の処理手順を示すシーケンス図である。なお、図２７の処理を開始する前提として、シンク機器とソース機器との間でDTCP認証・鍵交換処理が行われており、シンク機器はソース機器のMACアドレスを事前に取得しているものとする。

【０１３４】

まず、シンク機器はソース機器にMACアドレス検索事前通知を送信する（ステップＳ７１）とともに、ソース機器のIPアドレスからMACアドレス検索を行う（ステップＳ７２）。

【０１３５】

ソース機器は、シンク機器からのMACアドレス検索を受信すると（ステップＳ７３）、自機器のMACアドレスをシンク機器に送信する（ステップＳ７４）。

【０１３６】

シンク機器は、ソース機器から送信されたMACアドレスと事前に取得しているソース機器のMACアドレスとが一致するか否かを比較判定し（ステップＳ７５）、両者が一致すれば、ソース機器からのコンテンツを受信する（ステップＳ７６）。

【０１３７】

ソース機器は、シンク機器からのMACアドレス検索要求を受信したか否かを判定し（ステップＳ７７）、受信した場合にはコンテンツの受信を継続して行い（ステップＳ７８）、受信しなかった場合には所定のエラー処理を行って、コンテンツの受信を中止する。

【０１３８】

図２８はソース機器とシンク機器が物理的に同一のセグメントに存在しない場合における第５の実施形態の処理手順を示すシーケンス図である。この場合、シンク機器と同一のセグメントにはソース機器は接続されていないため、シンク機器から上位のプロトコルで送信されたMACアドレス検索事前通知はソース機器に届くが（ステップＳ８１）、ソース機器のIPアドレスからMACアドレスを検索しようとしても（ステップＳ８２）、VPNサーバ機器が代理で応答してしまう（ステップＳ８３）。

【０１３９】

仮にVPNサーバ機器のMACアドレスがソース機器のMACアドレスと同一であったとすると、シンク機器でのMACアドレス比較結果は一致し（ステップＳ８４）、ソース機器はシンク機器にコンテンツを送信してしまう（ステップＳ８５）。

【０１４０】

ところが、ソース機器はIPアドレスからのMACアドレス検索を受信していないため（ステップＳ８６）、コンテンツの送信を中止する（ステップＳ８７）。

【０１４１】

このように、第５の実施形態では、シンク機器と同一セグメントに接続されているVPNサーバ機器がソース機器と同一のMACアドレスであっても、ソース機器が同一セグメントに接続されていない限り、コンテンツの送信を確実に中止できる。

【０１４２】

（第６の実施形態）

第６の実施形態は、ソース機器がシンク機器からのMACアドレス検索事前通知を受けると、それに対する応答をシンク機器に送信するようにしたものである。

【０１４３】

図２９はソース機器の第６の実施形態の内部構成を示すブロック図である。図２９のソース機器は、図２５のソース機器の構成に加えて、MACアドレス検索事前通知応答をシンク機器に送信する制御を行うMACアドレス検索事前通知応答処理部６５を有する。

【０１４４】

図３０はシンク機器の第６の実施形態の内部構成を示すブロック図である。図３０のシンク機器は、図２６のシンク機器の構成に加えて、ソース機器からのMACアドレス検索事前通知応答を受信する制御を行うMACアドレス検索事前通知応答受信処理部６４を有する。

【０１４５】

図３１はソース機器とシンク機器が物理的に同一のセグメントに存在する場合における第６の実施形態の処理手順を示すシーケンス図である。なお、図３１の処理を開始する前提として、シンク機器とソース機器との間でDTCP認証・鍵交換処理が行われており、シンク機器はソース機器のMACアドレスを事前に取得しているものとする。

【０１４６】

以下では、図２７と異なる処理を中心に説明する。ソース機器は、シンク機器

からのMACアドレス検索事前通知を受信すると（ステップＳ９１）、それに対する応答（MACアドレス検索事前通知応答）をシンク機器に送信する（ステップＳ９３）。

【０１４７】

シンク機器は、ソース機器からのMACアドレス検索事前通知応答を受信し（ステップＳ９５）、MACアドレスの比較処理を行う（ステップＳ９６）。次に、シンク機器はMACアドレス検索事前通知応答を受信したか否かを判定し（ステップＳ９７）、受信した場合にはソース機器からのコンテンツ送信を受ける（ステップＳ９８）。

【０１４８】

図３２はソース機器とシンク機器が物理的に同一のセグメントに存在しない場合における第６の実施形態の処理手順を示すシーケンス図である。シンク機器は上位のプロトコルを用いてMACアドレス検索事前通知をソース機器に送信するため（ステップＳ１０１）、この通知をソース機器は受信できるが、シンク機器がソース機器のIPアドレスからMACアドレス検索を行うと（ステップＳ１０２）、シンク機器と同一セグメントに位置するVPNサーバ機器がMACアドレスを代理で応答する（ステップＳ１０３）。

【０１４９】

VPNサーバ機器のMACアドレスがソース機器のMACアドレスと同一であれば、シンク機器でのMACアドレス比較結果は一致するが（ステップＳ１０４）、シンク機器はソース機器からのMACアドレス検索事前通知応答を受信していないため（ステップＳ１０５）、ソース機器に対してコンテンツ送信の中止を依頼し（ステップＳ１０６）、これにより、ソース機器はコンテンツ送信を中止する（ステップＳ１０７）。

【０１５０】

このように、第６の実施形態では、シンク機器からソース機器に送信したMACアドレス検索事前通知に対する応答がシンク機器で受信された場合のみ、コンテンツ送信を行うようにしたため、シンク機器とソース機器とが同一のセグメントに位置する場合のみコンテンツ送信を行うことができる。

【０１５１】

【発明の効果】

以上詳細に説明したように、本発明によれば、機器識別情報検索手段で検索された機器識別情報と機器識別情報登録手段に登録されている機器識別情報とが一致する場合のみ、対応する受信装置へのコンテンツの送信を許可するため、限られた受信装置のみにコンテンツを提供でき、コンテンツの不正受信を防止できる。

【０１５２】

これにより、同じサブネットの複数の受信装置のうち、物理的に同一のサブネットに接続されている受信装置と、仮想的に同一のサブネットに接続されている受信装置とを区別して、前者と後者でコンテンツの配布条件を変えることができる。

【０１５３】

また、本発明によれば、送信装置からの機器時期別情報検索要求を受信装置が受信したか否かを確認することにより、送信装置と受信装置とが同一のセグメントに接続されているか否かを簡易かつ正確に判断できる。

【図面の簡単な説明】

【図１】

本発明に係るコンテンツ送受信システムの第１の実施形態の概略構成を示すブロック図。

【図２】

ソース機器Ａの内部構成の一例を示すブロック図。

【図３】

MACアドレステーブルの構造を示す図。

【図４】

シンク機器Ｂ，Ｃの内部構成の一例を示すブロック図。

【図５】

本実施形態の通信システムの処理手順を示す図。

【図６】

本実施形態の通信システムの処理手順を示す図。

【図７】

ソース機器Ａの処理手順を示す図。

【図８】

ソース機器とシンク機器との間にＶＰＮサーバ機器が接続されているコンテンツ送受信システムの概略構成を示すブロック図。

【図９】

本発明に係るコンテンツ送受信システムの第２の実施形態の概略構成を示すブロック図。

【図１０】

VPNサーバ機器ＦとVPNクライアント機器Ｇが二つのネットワークをトンネリングするコンテンツ送受信システムのブロック構成を示す図。

【図１１】

図１０で示したコンテンツ送受信システムの形態におけるソース機器の内部構成を示すブロック図。

【図１２】

図１０で示したコンテンツ送受信システムの形態におけるシンク機器の内部構成を示すブロック図。

【図１３】

シンク機器の内部でMACアドレスの比較を行う場合のソース機器の内部構成を示すブロック図。

【図１４】

シンク機器の内部でMACアドレスの比較を行う場合のシンク機器の内部構成を示すブロック図。

【図１５】

VPN機器の接続形態の種類を示す図。

【図１６】

本発明に係るコンテンツ送受信システムの第３の実施形態の概略構成を示すブロック図。

【図１７】

第３の実施形態におけるソース機器A15の内部構成を示すブロック図。

【図１８】

第３の実施形態におけるシンク機器B11,C12の内部構成を示すブロック図。

【図１９】

第３の実施形態の処理手順を示すシーケンス図。

【図２０】

ソース機器とシンク機器が物理的に同一のセグメントに存在しない場合における第３の実施形態の処理手順を示すシーケンス図。

【図２１】

ソース機器の第４の実施形態の内部構成を示すブロック図。

【図２２】

シンク機器の第４の実施形態の内部構成を示すブロック図。

【図２３】

第４の実施形態の処理手順を示すシーケンス図。

【図２４】

ソース機器とシンク機器が物理的に同一のセグメントに存在しない場合における第４の実施形態の処理手順を示すシーケンス図。

【図２５】

ソース機器の第５の実施形態の内部構成を示すブロック図。

【図２６】

シンク機器の第５の実施形態の内部構成を示すブロック図。

【図２７】

ソース機器とシンク機器が物理的に同一のセグメントに存在する場合における第５の実施形態の処理手順を示すシーケンス図。

【図２８】

ソース機器とシンク機器が物理的に同一のセグメントに存在しない場合における第５の実施形態の処理手順を示すシーケンス図。

【図２９】

ソース機器の第６の実施形態の内部構成を示すブロック図。

【図３０】

シンク機器の第６の実施形態の内部構成を示すブロック図。

【図３１】

ソース機器とシンク機器が物理的に同一のセグメントに存在する場合における第６の実施形態の処理手順を示すシーケンス図。

【図３２】

ソース機器とシンク機器が物理的に同一のセグメントに存在しない場合における第６の実施形態の処理手順を示すシーケンス図。

【図３３】

送信装置と受信装置を備えた従来のネットワークシステムの全体構成を示すブロック図。

【図３４】

インターネットセグメントＡ，Ｂにそれぞれ別個のシンク機器が接続されているネットワークシステムの全体構成を示すブロック図。

【図３５】

ソース機器とシンク機器のネットワークアドレスが同一か否かを判別する処理手順を示すフローチャート。

【図３６】

VPNを使ったネットワーク構成の一例を示す図。

【符号の説明】

１０　イーサネットセグメントＡ

１１　シンク機器Ｂ

１２　シンク機器Ｃ

１３　ルータ機器Ｆ

１４　インターネット

１５　ソース機器Ａ

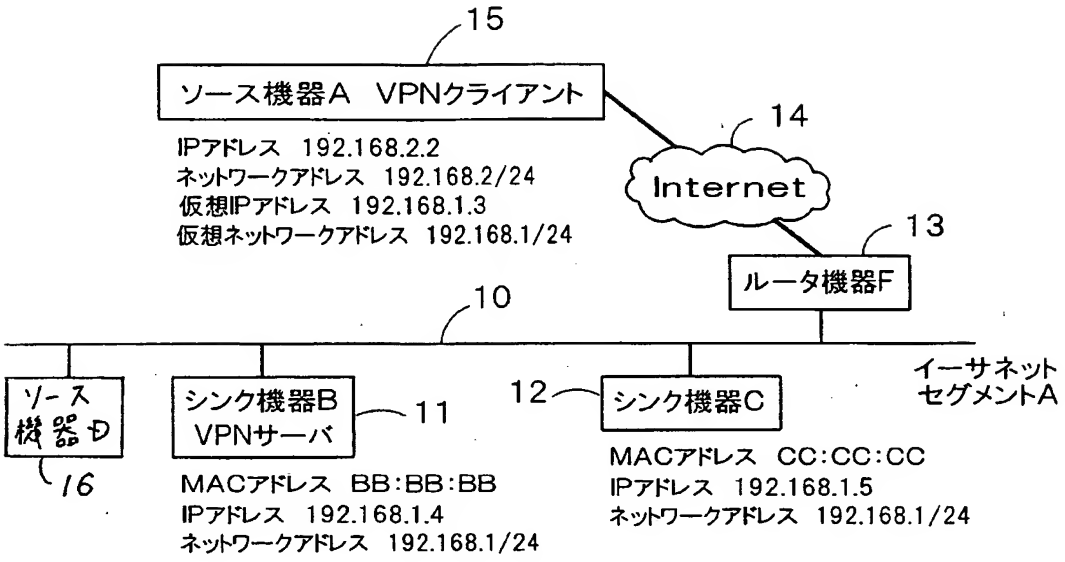
２１　ネットワークインタフェース部

２２　通信処理部

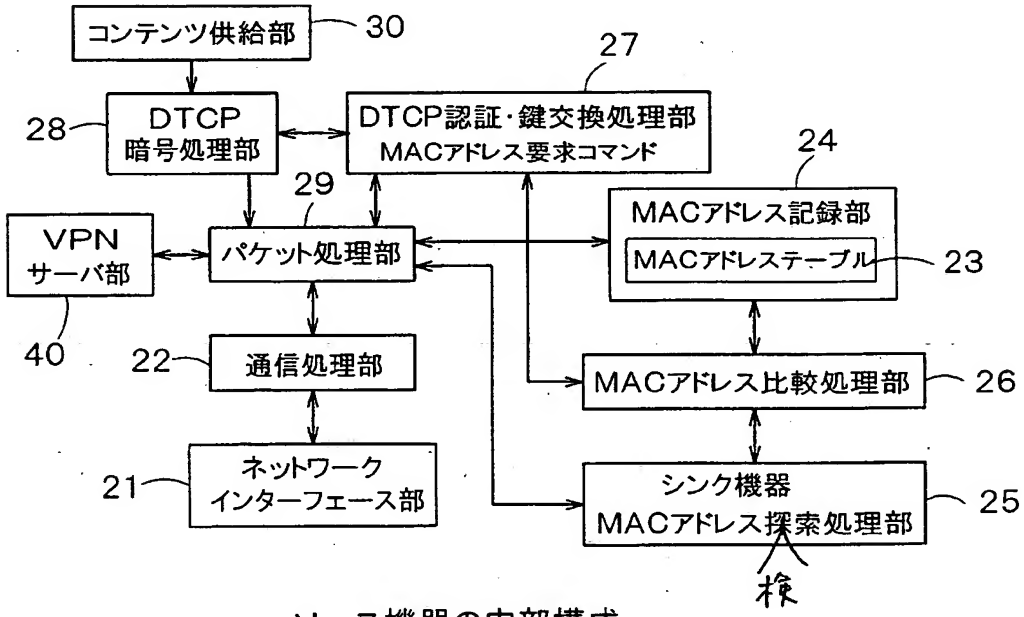
２３　MACアドレステーブル
２４　MACアドレス記録部
２５　シンク機器MACアドレス検索処理部
２６　MACアドレス比較処理部
２７　DTCP認証・鍵交換処理部
２８　DTCP暗号処理部
２９　パケット処理部
３０　コンテンツ供給部
３１　ネットワークインタフェース部
３２　通信処理部
３３　MACアドレス送信部
３４　VPNクライアント部
３５　DTCP認証・鍵交換処理部
３６　DTCP暗号処理部
３７　パケット処理部
３８　コンテンツ処理部
６２　MACアドレス検索事前通知処理部
６３　MACアドレス検索事前通知受信処理部
６４　MACアドレス検索事前通知応答受信処理部
６５　MACアドレス検索事前通知応答処理部

【書類名】　図面

【図１】



【図２】



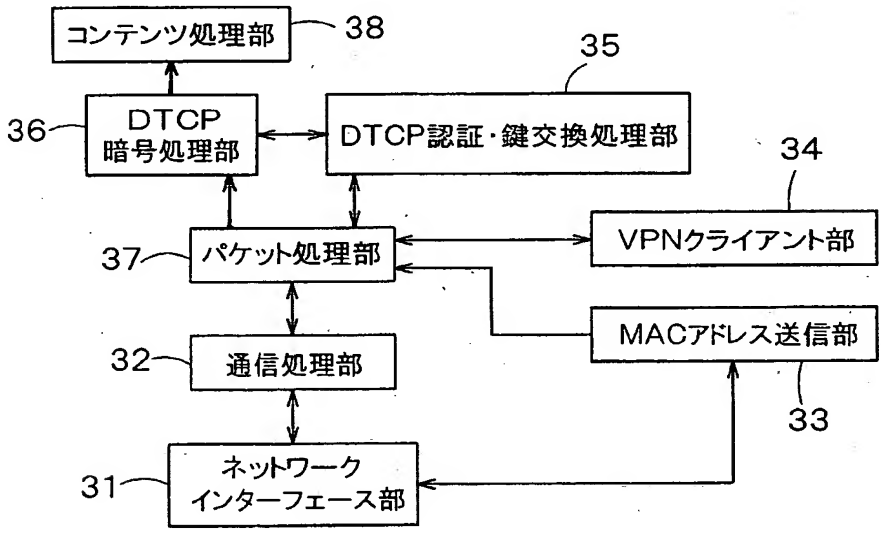
ソース機器の内部構成

【図３】

MACアドレステーブル

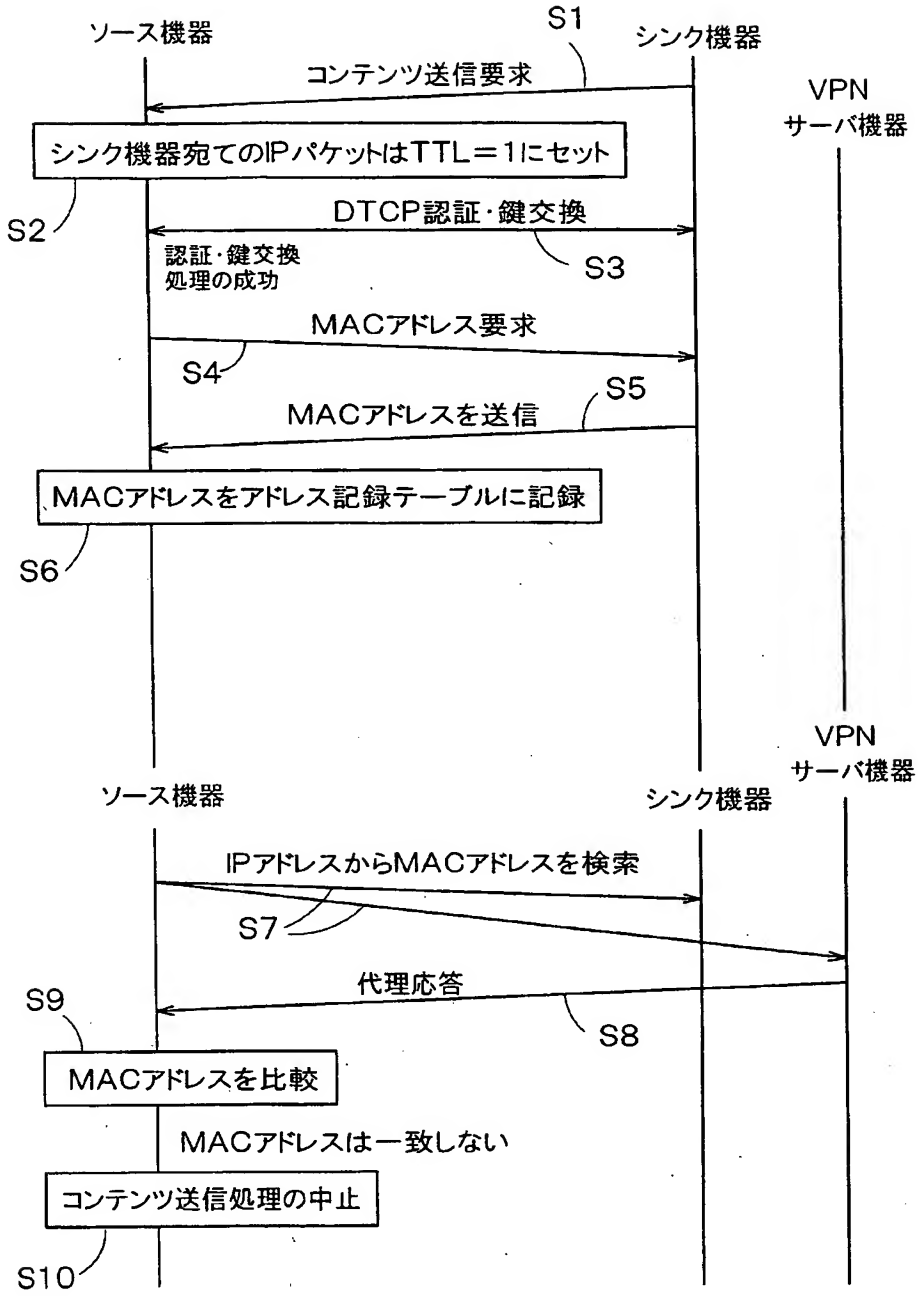
	IPアドレス	MACアドレス	デバイスID
シンク機器B	192.168.1.3	BB:BB:BB	B1
シンク機器C	192.168.1.5	CC:CC:CC	C1
シンク機器X	192.168.78	XX:XX:XX	X1
••••			

【図４】

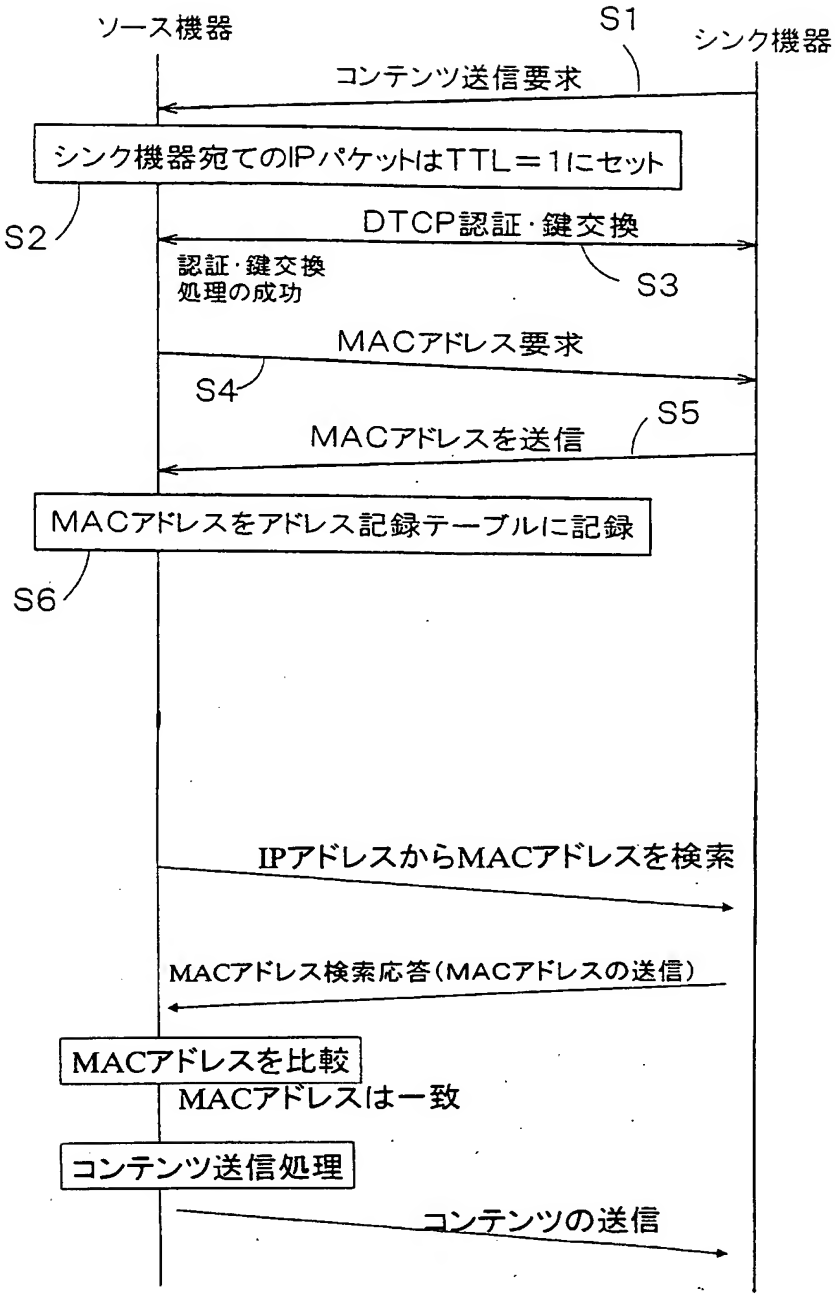


シンク機器の内部構成

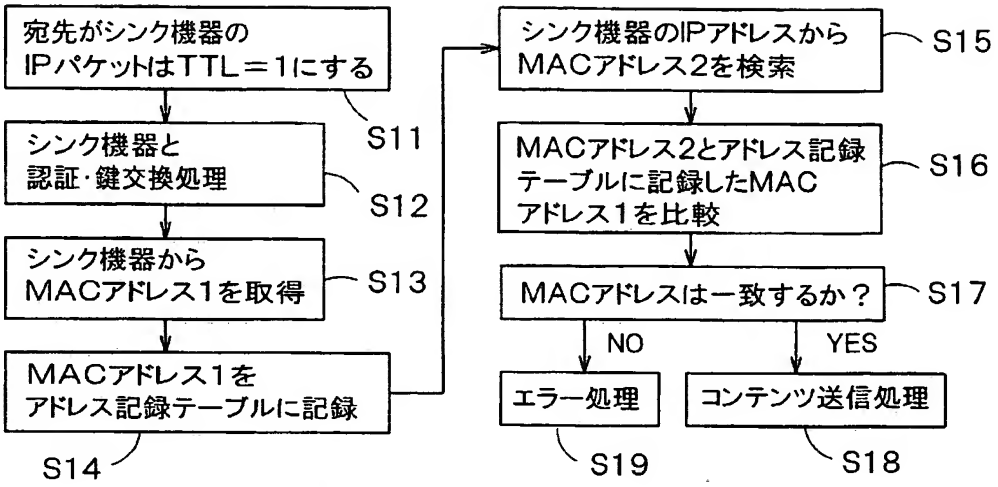
【図５】


ソース機器
S1
シンク機器
コンテンツ送信要求
VPN
サーバ機器
シンク機器宛てのIPパケットはTTL＝1にセット
S2
DTCP認証・鍵交換
S3
認証・鍵交換
処理の成功
MACアドレス要求
S4
S5
MACアドレスを送信
MACアドレスをアドレス記録テーブルに記録
S6
VPN
サーバ機器
ソース機器
シンク機器
IPアドレスからMACアドレスを検索
S7
代理応答
S9
S8
MACアドレスを比較
MACアドレスは一致しない
コンテンツ送信処理の中止
S10

【図６】

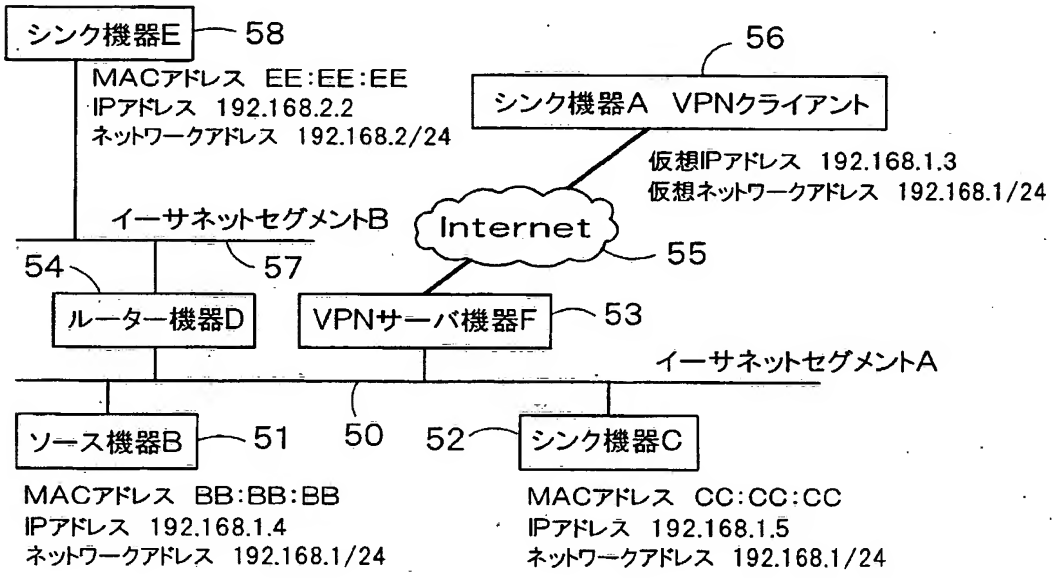

ソース機器
S1
シンク機器
コンテンツ送信要求
シンク機器宛てのIPパケットはTTL＝1にセット
S2
DTCP認証・鍵交換
認証・鍵交換
処理の成功
S3
MACアドレス要求
S4
S5
MACアドレスを送信
MACアドレスをアドレス記録テーブルに記録
S6
IPアドレスからMACアドレスを検索
MACアドレス検索応答（MACアドレスの送信）
MACアドレスを比較
MACアドレスは一致
コンテンツ送信処理
コンテンツの送信

【図７】

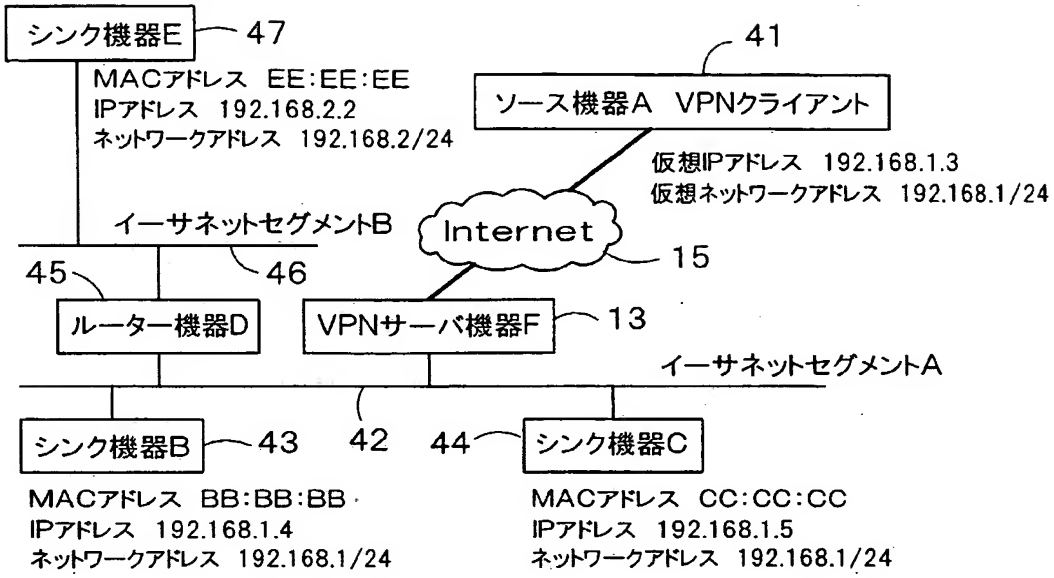


ソース機器の処理手順

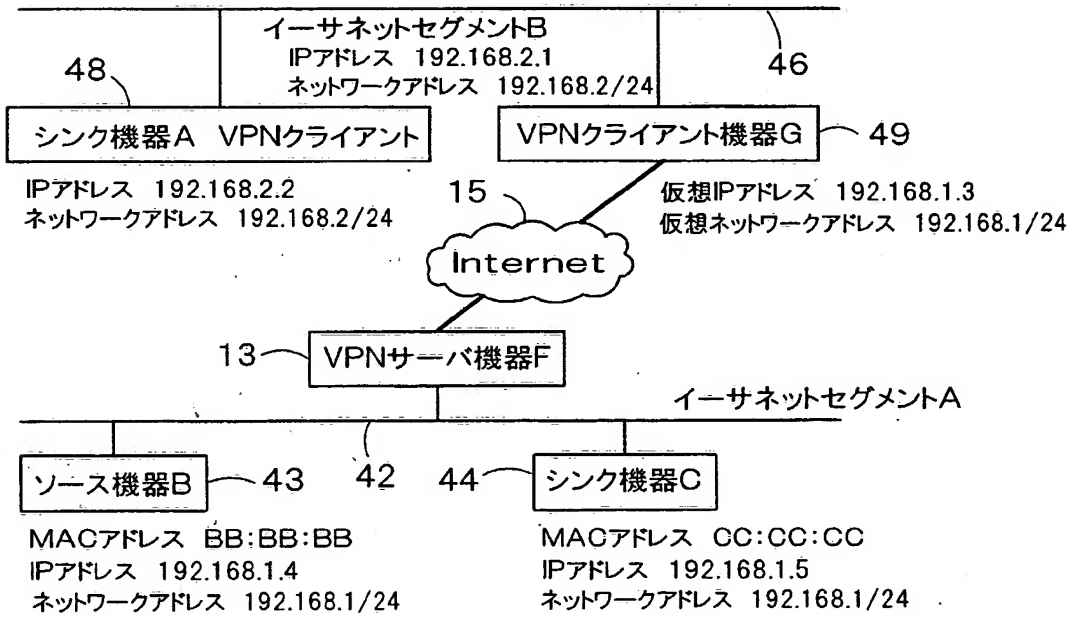
【図８】



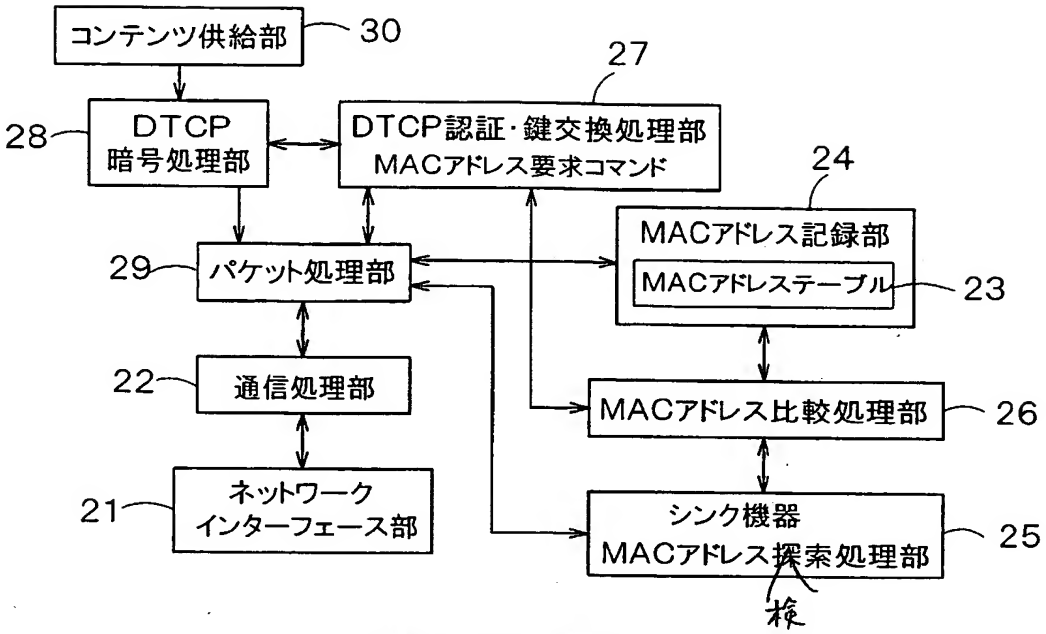
【図９】


シンク機器E
47
MACアドレス EE:EE:EE
IPアドレス 192.168.2.2
ネットワークアドレス 192.168.2/24
41
ソース機器A VPNクライアント
仮想IPアドレス 192.168.1.3
仮想ネットワークアドレス 192.168.1/24
イーサネットセグメントB
Internet
15
45
46
ルーター機器D
VPNサーバ機器F
13
イーサネットセグメントA
シンク機器B
43
42
44
シンク機器C
MACアドレス BB:BB:BB
IPアドレス 192.168.1.4
ネットワークアドレス 192.168.1/24
MACアドレス CC:CC:CC
IPアドレス 192.168.1.5
ネットワークアドレス 192.168.1/24

【図１０】

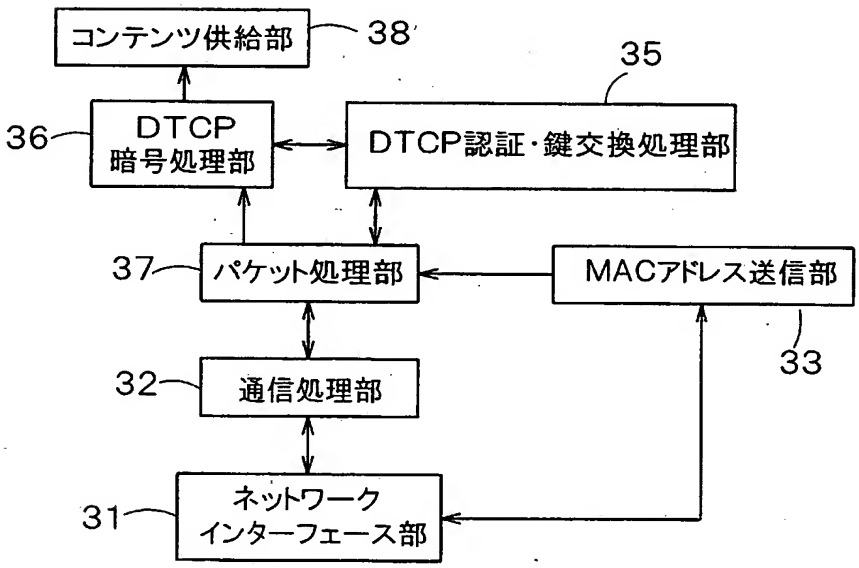

イーサネットセグメントB
IPアドレス 192.168.2.1
ネットワークアドレス 192.168.2/24
48
46
シンク機器A VPNクライアント
VPNクライアント機器G
49
IPアドレス 192.168.2.2
ネットワークアドレス 192.168.2/24
15
仮想IPアドレス 192.168.1.3
仮想ネットワークアドレス 192.168.1/24
Internet
13
VPNサーバ機器F
イーサネットセグメントA
ソース機器B
43
42
44
シンク機器C
MACアドレス BB:BB:BB
IPアドレス 192.168.1.4
ネットワークアドレス 192.168.1/24
MACアドレス CC:CC:CC
IPアドレス 192.168.1.5
ネットワークアドレス 192.168.1/24

【図１１】



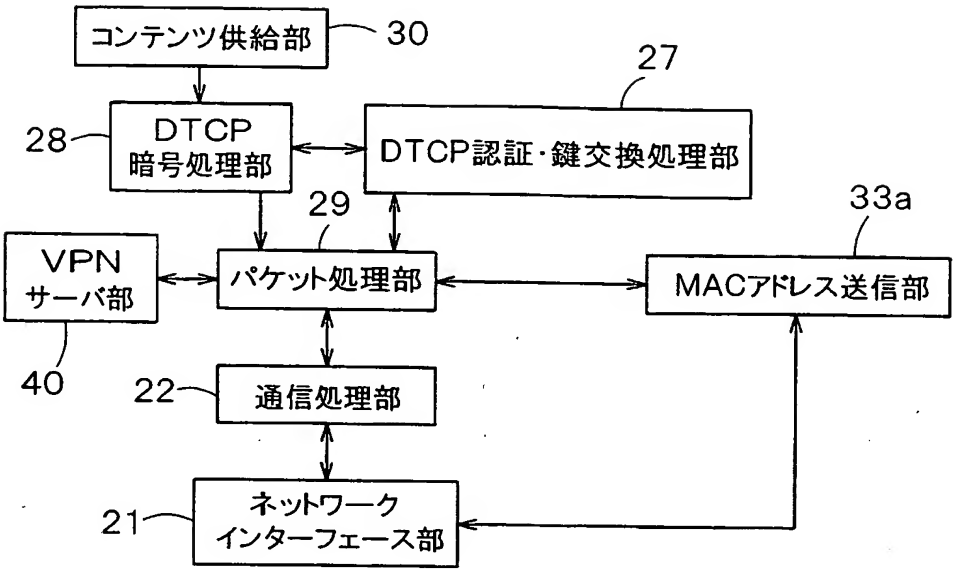
ソース機器の内部構成

【図１２】



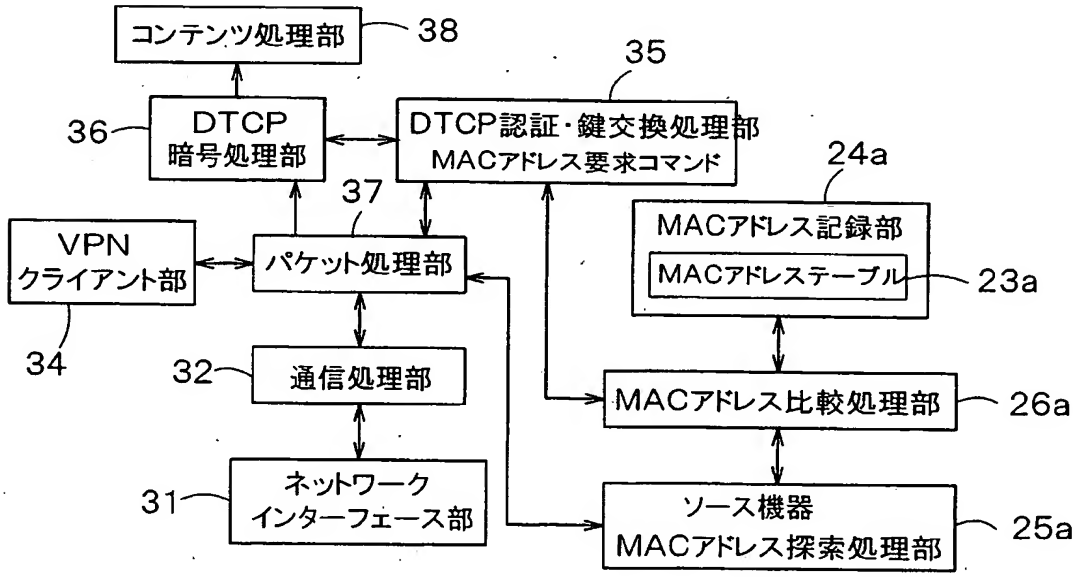
シンク機器の内部構成

【図１３】



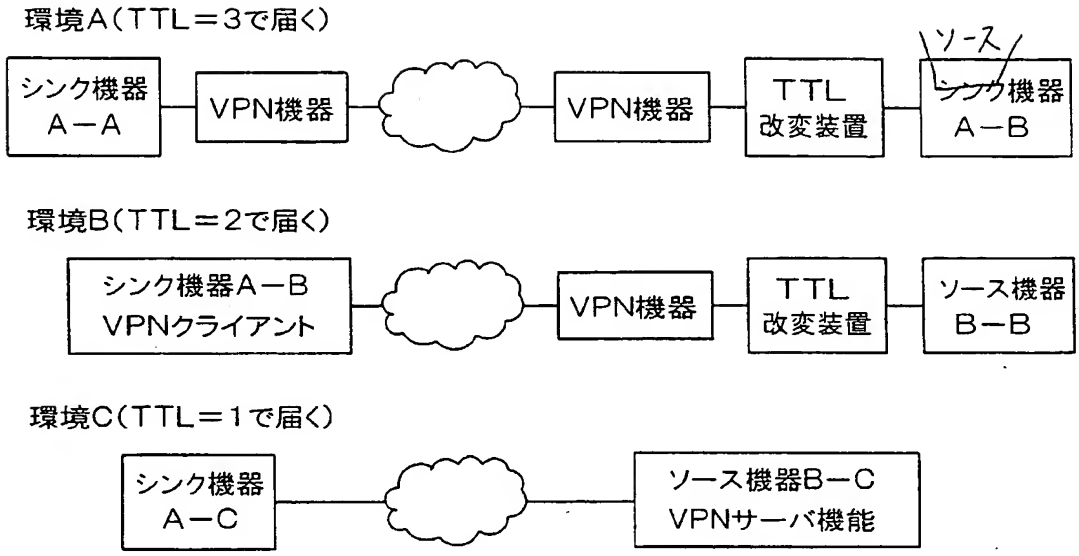
ソース機器の内部構成

【図１４】

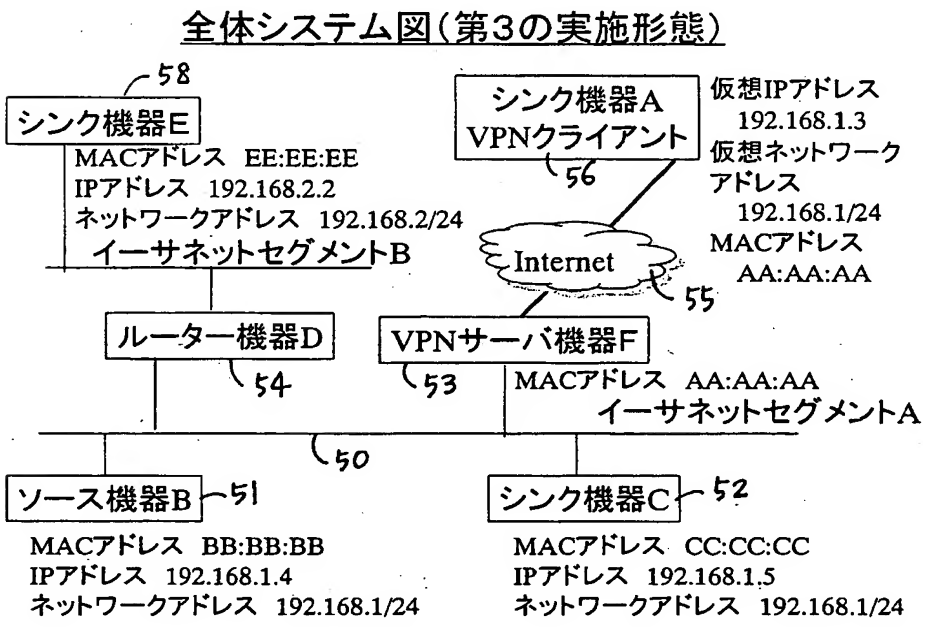


シンク機器の内部構成

【図１５】

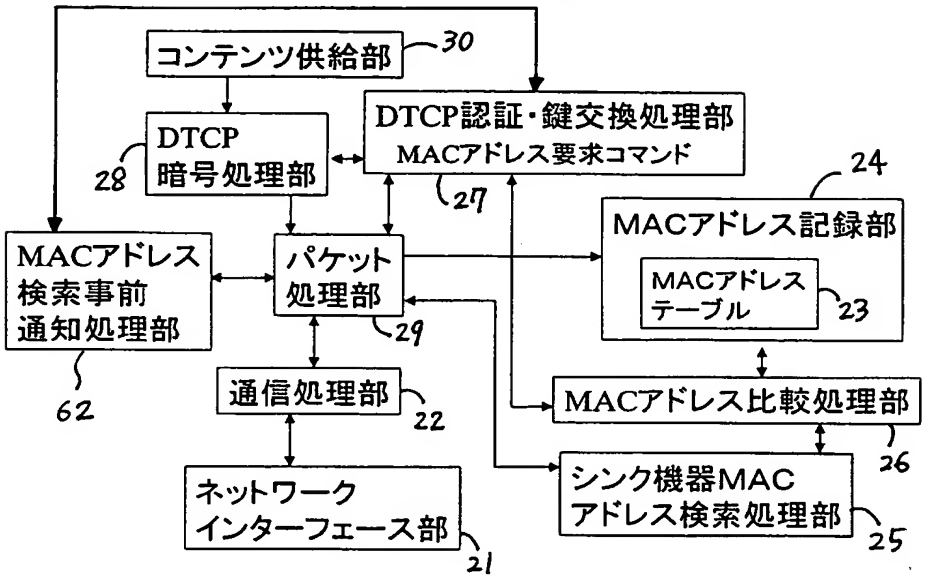

環境A（TTL＝3で届く）
シンク機器
A－A
VPN機器
VPN機器
TTL
改変装置
ソース
シンク機器
A－B
環境B（TTL＝2で届く）
シンク機器A－B
VPNクライアント
VPN機器
TTL
改変装置
ソース機器
B－B
環境C（TTL＝1で届く）
シンク機器
A－C
ソース機器B－C
VPNサーバ機能

【図１６】


全体システム図（第3の実施形態）
58
シンク機器E
MACアドレス EE:EE:EE
IPアドレス 192.168.2.2
ネットワークアドレス 192.168.2/24
イーサネットセグメントB
シンク機器A
VPNクライアント
56
仮想IPアドレス
192.168.1.3
仮想ネットワーク
アドレス
192.168.1/24
MACアドレス
AA:AA:AA
Internet
55
ルーター機器D
54
VPNサーバ機器F
53
MACアドレス AA:AA:AA
イーサネットセグメントA
50
ソース機器B
51
シンク機器C
52
MACアドレス BB:BB:BB
IPアドレス 192.168.1.4
ネットワークアドレス 192.168.1/24
MACアドレス CC:CC:CC
IPアドレス 192.168.1.5
ネットワークアドレス 192.168.1/24

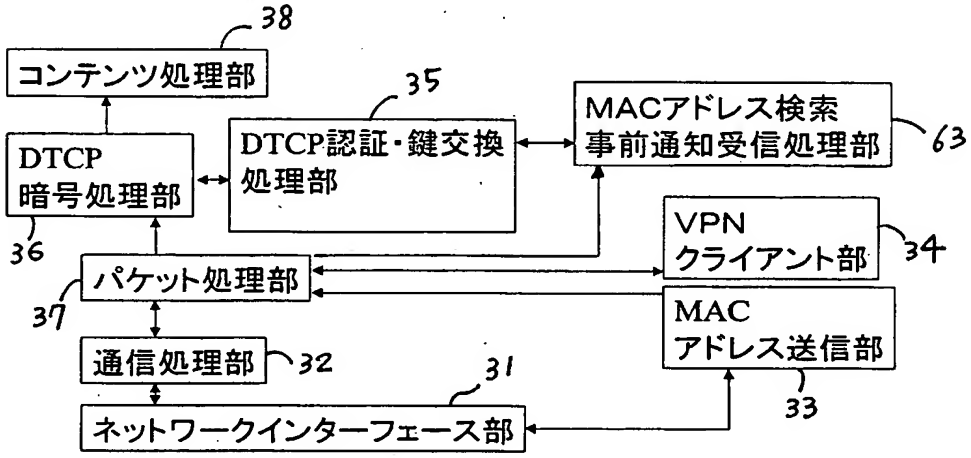
【図１７】

ソース機器（第3の実施形態）

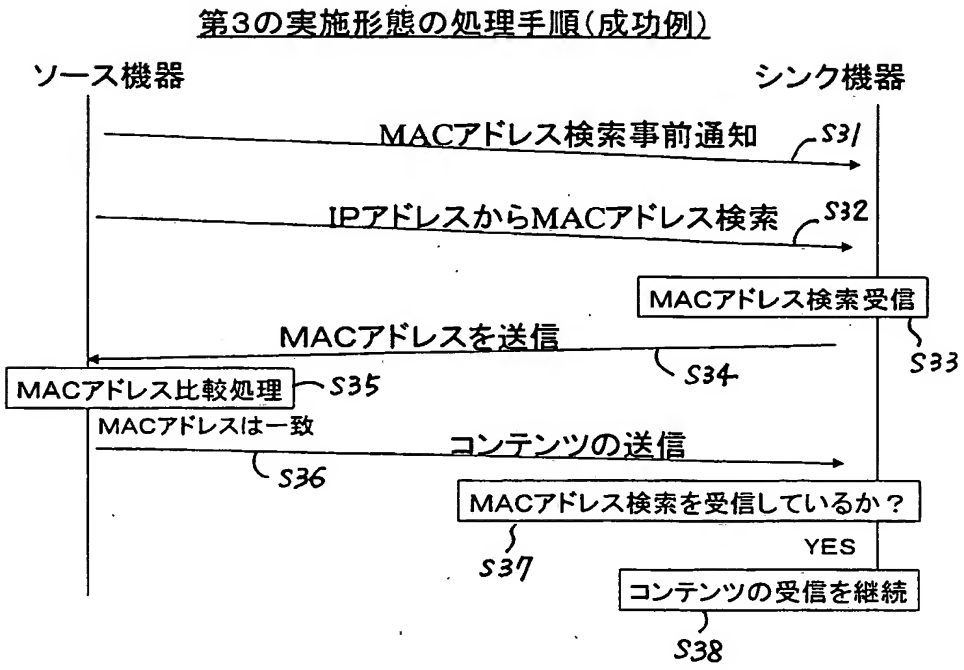


【図１８】

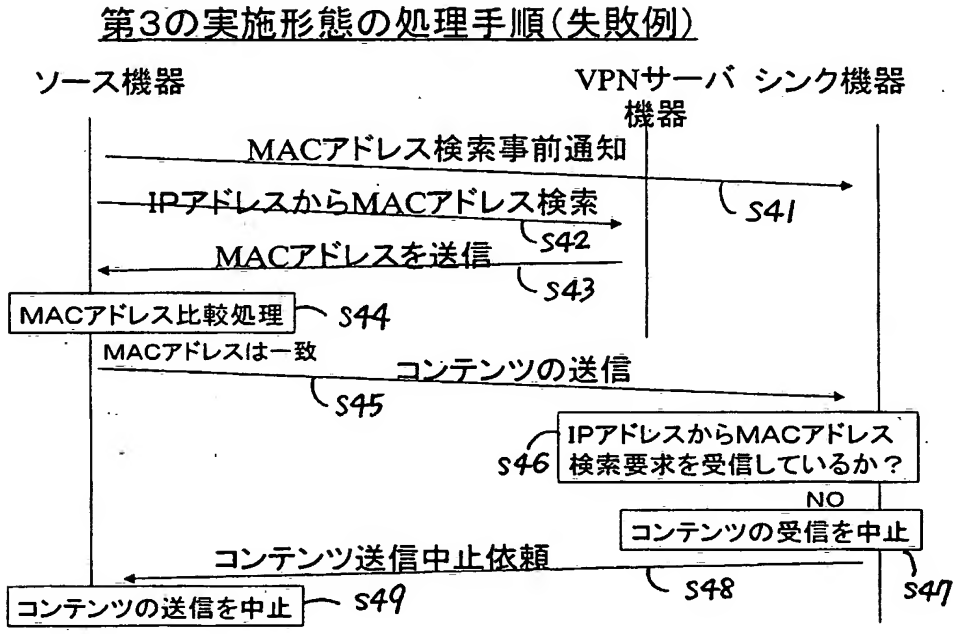
シンク機器（第3の実施形態）



【図１９】

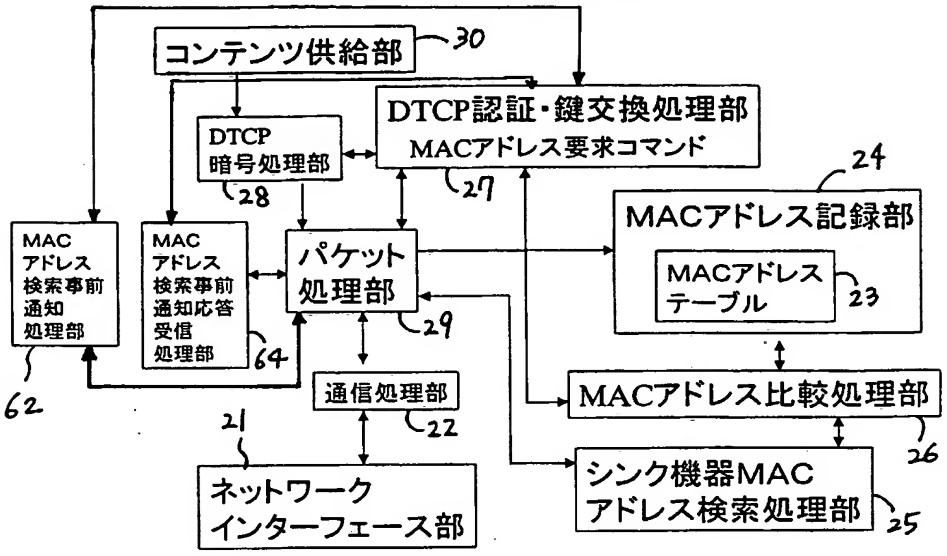

第3の実施形態の処理手順(成功例)
ソース機器
シンク機器
MACアドレス検索事前通知
S31
IPアドレスからMACアドレス検索
S32
MACアドレス検索受信
S33
MACアドレスを送信
S34
MACアドレス比較処理
S35
MACアドレスは一致
S36
コンテンツの送信
MACアドレス検索を受信しているか？
S37
YES
コンテンツの受信を継続
S38

【図２０】


第3の実施形態の処理手順(失敗例)
ソース機器
VPNサーバ
機器
シンク機器
MACアドレス検索事前通知
S41
IPアドレスからMACアドレス検索
S42
MACアドレスを送信
S43
MACアドレス比較処理
S44
MACアドレスは一致
コンテンツの送信
S45
S46
IPアドレスからMACアドレス
検索要求を受信しているか？
NO
コンテンツの受信を中止
S47
コンテンツ送信中止依頼
S48
コンテンツの送信を中止
S49

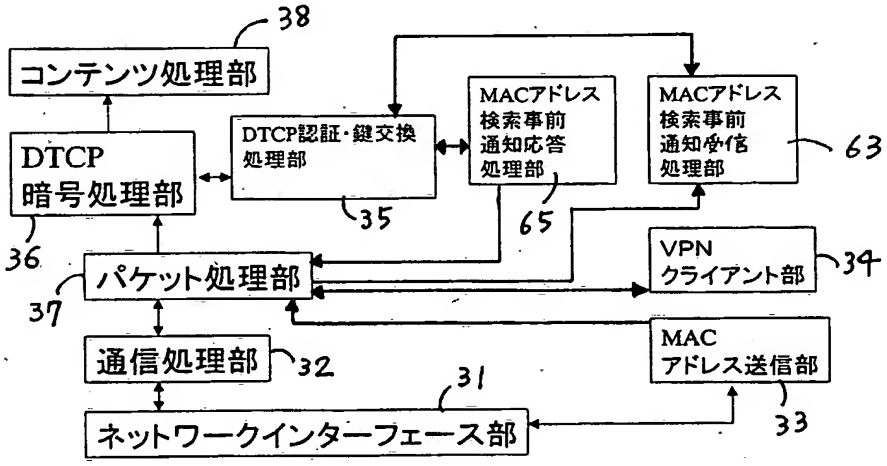
【図２１】

ソース機器（第４の実施形態）

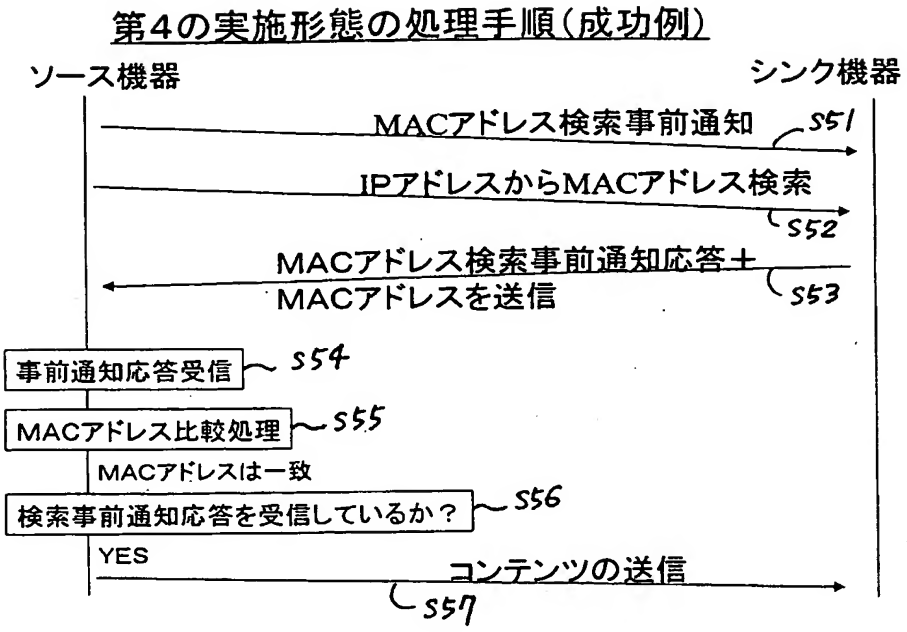


【図２２】

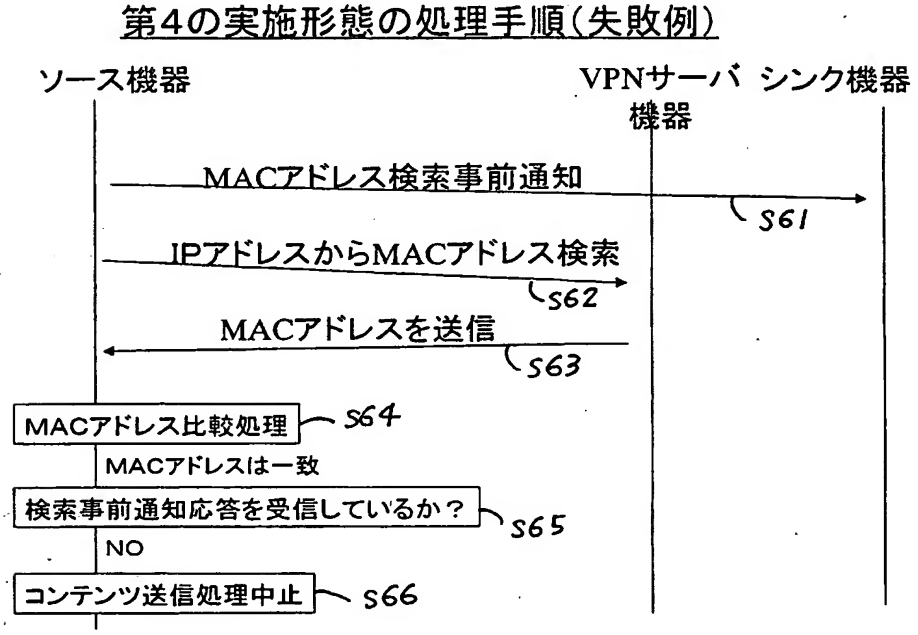
シンク機器（第４の実施形態）



【図２３】

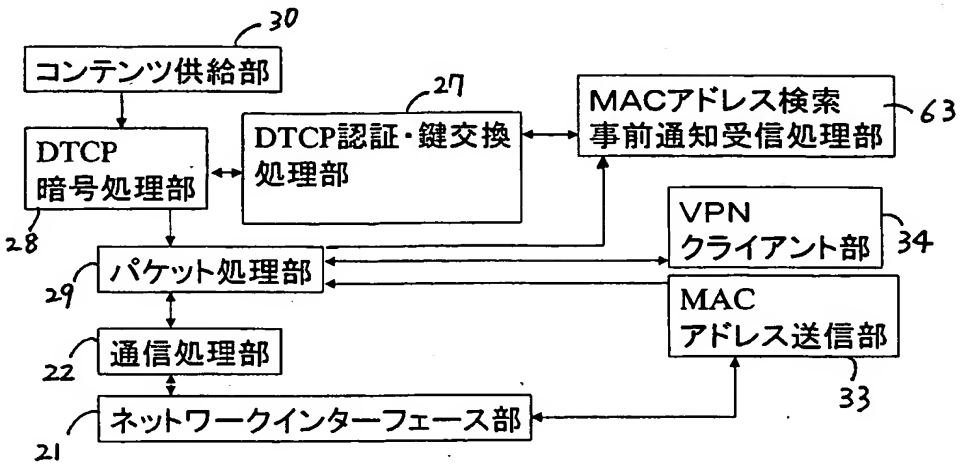

第4の実施形態の処理手順(成功例)
ソース機器
シンク機器
MACアドレス検索事前通知
S51
IPアドレスからMACアドレス検索
S52
MACアドレス検索事前通知応答＋
MACアドレスを送信
S53
事前通知応答受信
S54
MACアドレス比較処理
S55
MACアドレスは一致
検索事前通知応答を受信しているか？
S56
YES
コンテンツの送信
S57

【図２４】


第4の実施形態の処理手順(失敗例)
ソース機器
VPNサーバ
機器
シンク機器
MACアドレス検索事前通知
S61
IPアドレスからMACアドレス検索
S62
MACアドレスを送信
S63
MACアドレス比較処理
S64
MACアドレスは一致
検索事前通知応答を受信しているか？
S65
NO
コンテンツ送信処理中止
S66

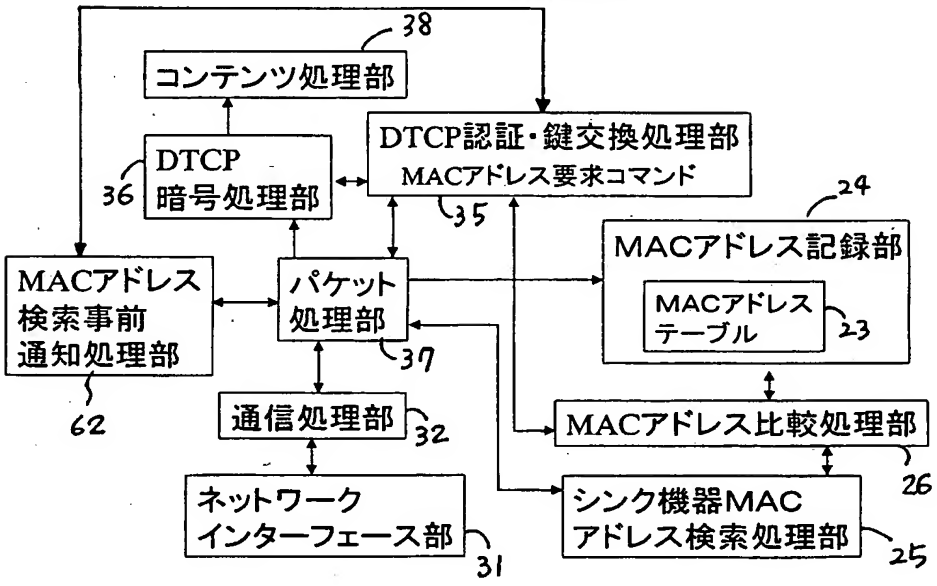
【図２５】

ソース機器（第5の実施形態）

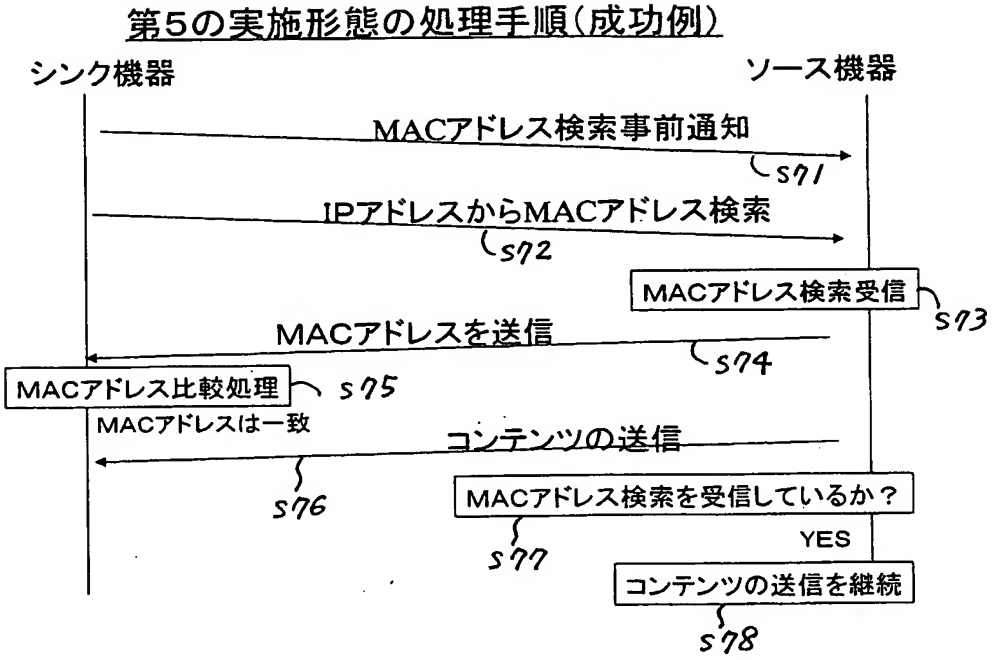


【図２６】

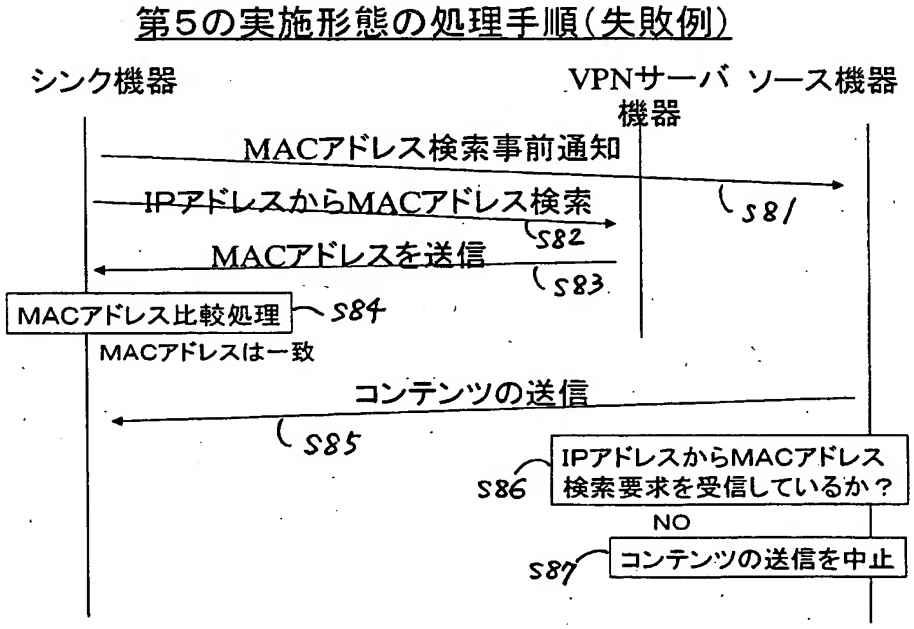
シンク機器（第5の実施形態）



【図２７】

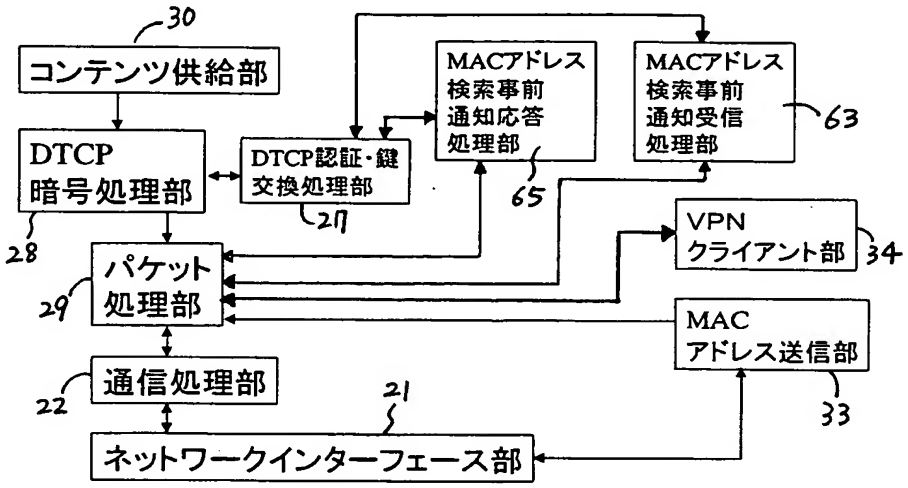

第5の実施形態の処理手順(成功例)
シンク機器
ソース機器
MACアドレス検索事前通知
S71
IPアドレスからMACアドレス検索
S72
MACアドレス検索受信
S73
MACアドレスを送信
S74
MACアドレス比較処理
S75
MACアドレスは一致
コンテンツの送信
S76
MACアドレス検索を受信しているか？
S77
YES
コンテンツの送信を継続
S78

【図２８】


第5の実施形態の処理手順(失敗例)
シンク機器
VPNサーバ機器
ソース機器
MACアドレス検索事前通知
S81
IPアドレスからMACアドレス検索
S82
MACアドレスを送信
S83
MACアドレス比較処理
S84
MACアドレスは一致
コンテンツの送信
S85
S86
IPアドレスからMACアドレス検索要求を受信しているか？
NO
S87
コンテンツの送信を中止

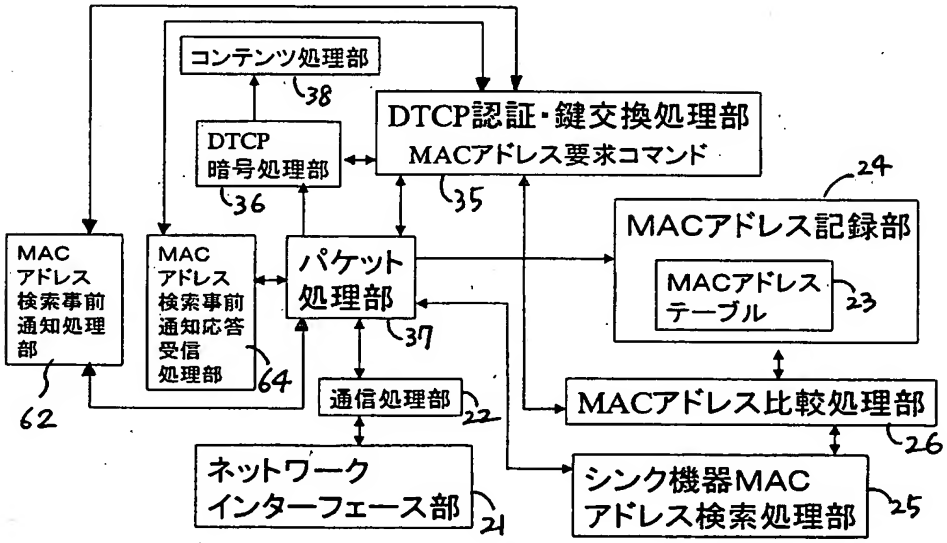
【図２９】

ソース機器（第６の実施形態）

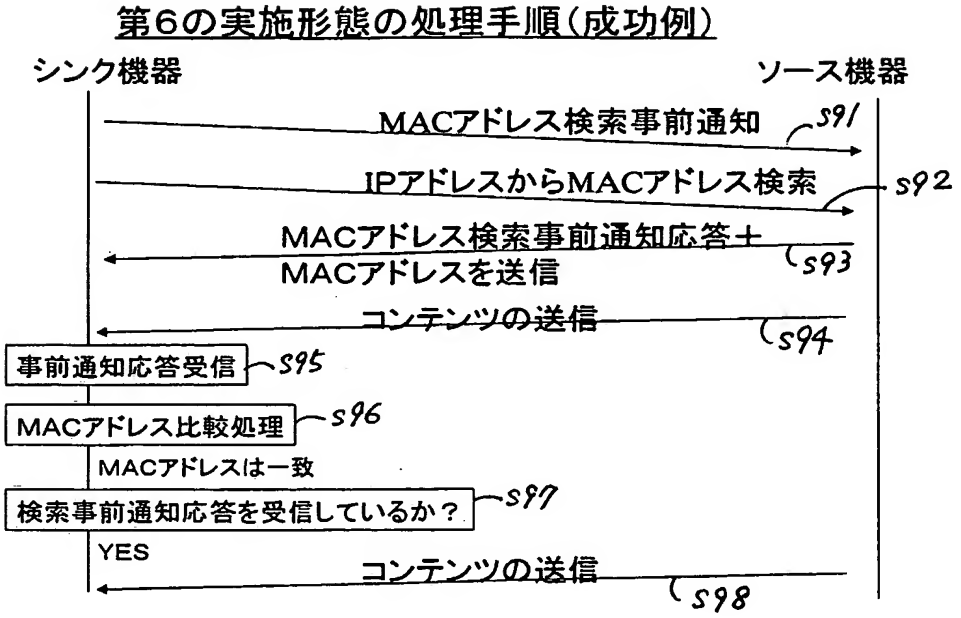


【図３０】

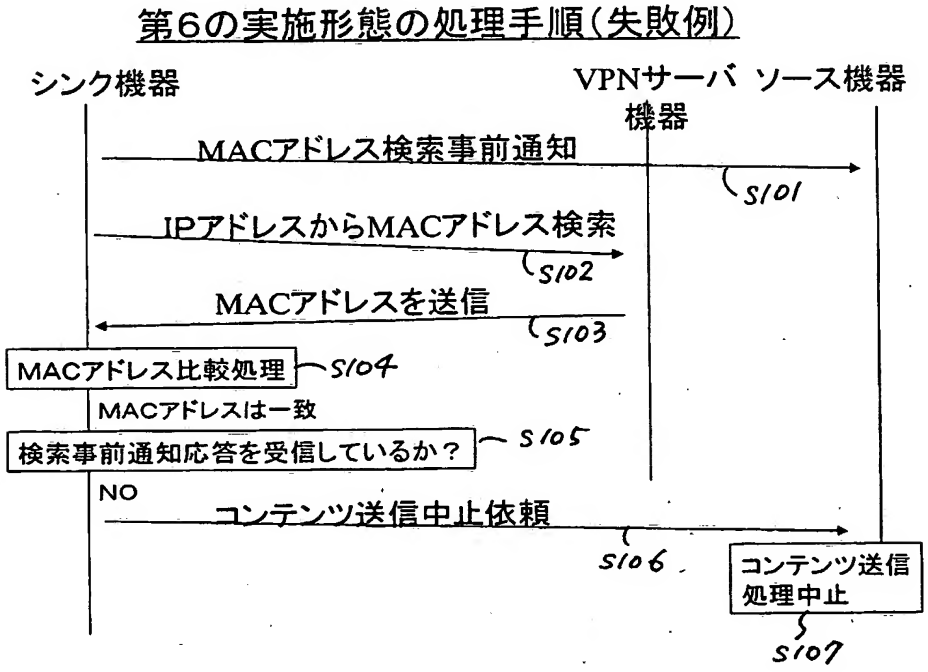
シンク機器（第６の実施形態）



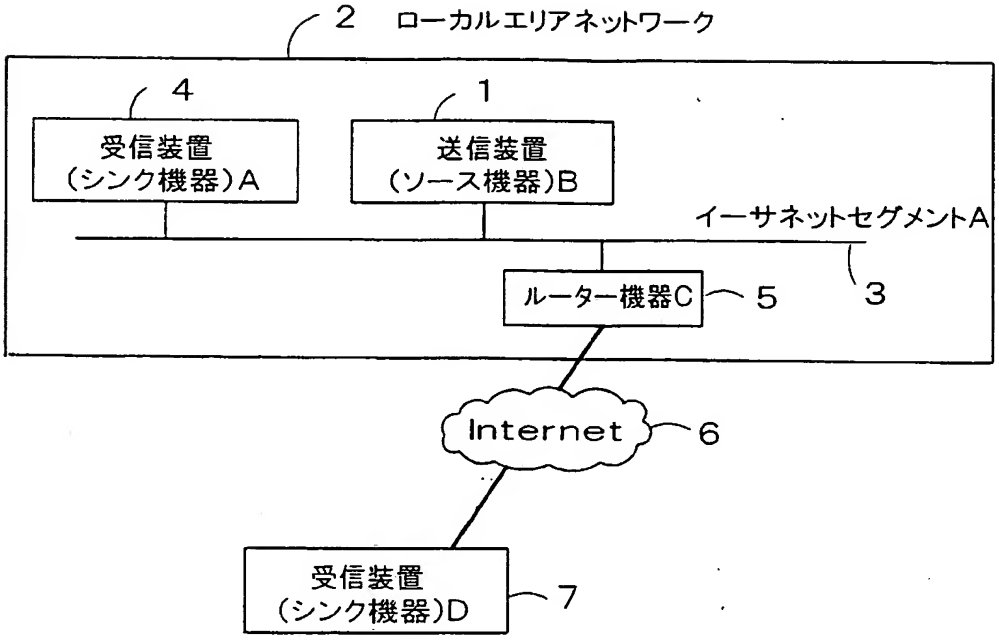
【図３１】


第6の実施形態の処理手順(成功例)
シンク機器
ソース機器
MACアドレス検索事前通知
S91
IPアドレスからMACアドレス検索
S92
MACアドレス検索事前通知応答＋
MACアドレスを送信
S93
コンテンツの送信
S94
事前通知応答受信
S95
MACアドレス比較処理
S96
MACアドレスは一致
検索事前通知応答を受信しているか？
S97
YES
コンテンツの送信
S98

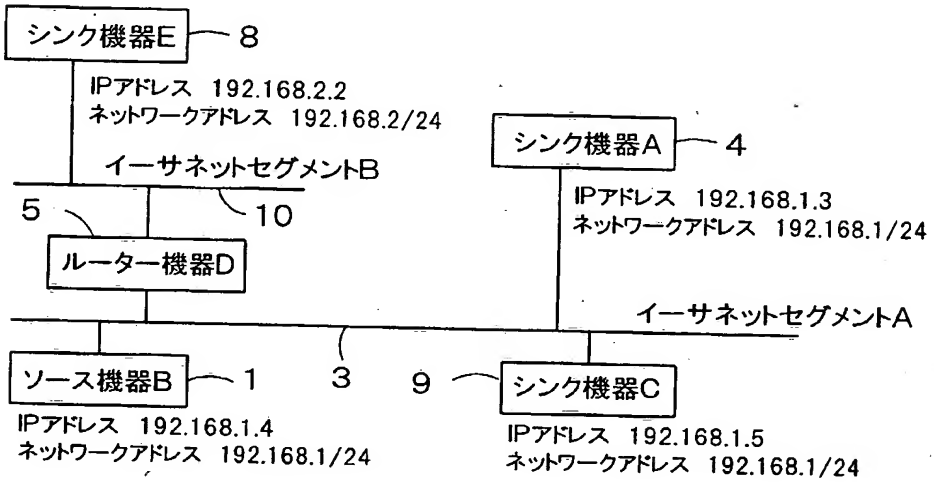
【図３２】


第6の実施形態の処理手順(失敗例)
シンク機器
VPNサーバ機器
ソース機器
MACアドレス検索事前通知
S101
IPアドレスからMACアドレス検索
S102
MACアドレスを送信
S103
MACアドレス比較処理
S104
MACアドレスは一致
検索事前通知応答を受信しているか？
S105
NO
コンテンツ送信中止依頼
S106
コンテンツ送信
処理中止
S107

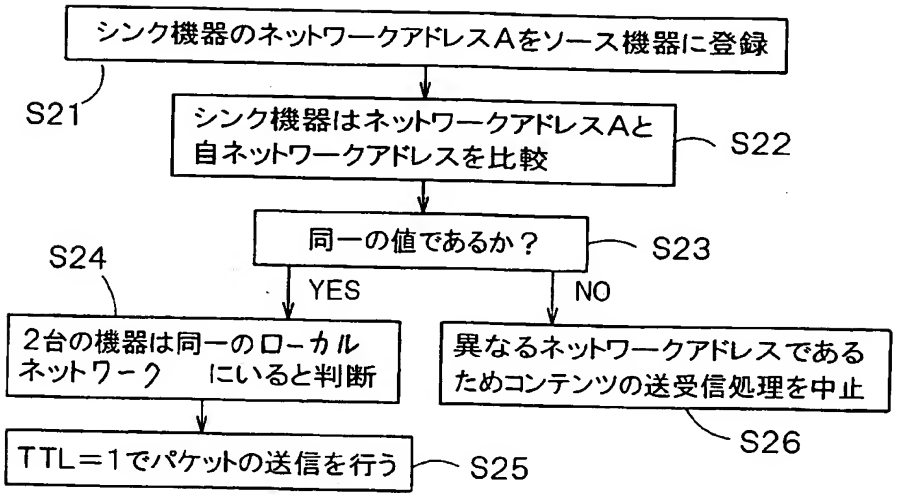
【図３３】


2　ローカルエリアネットワーク
4
受信装置
(シンク機器)A
1
送信装置
(ソース機器)B
イーサネットセグメントA
3
ルーター機器C
5
Internet
6
受信装置
(シンク機器)D
7

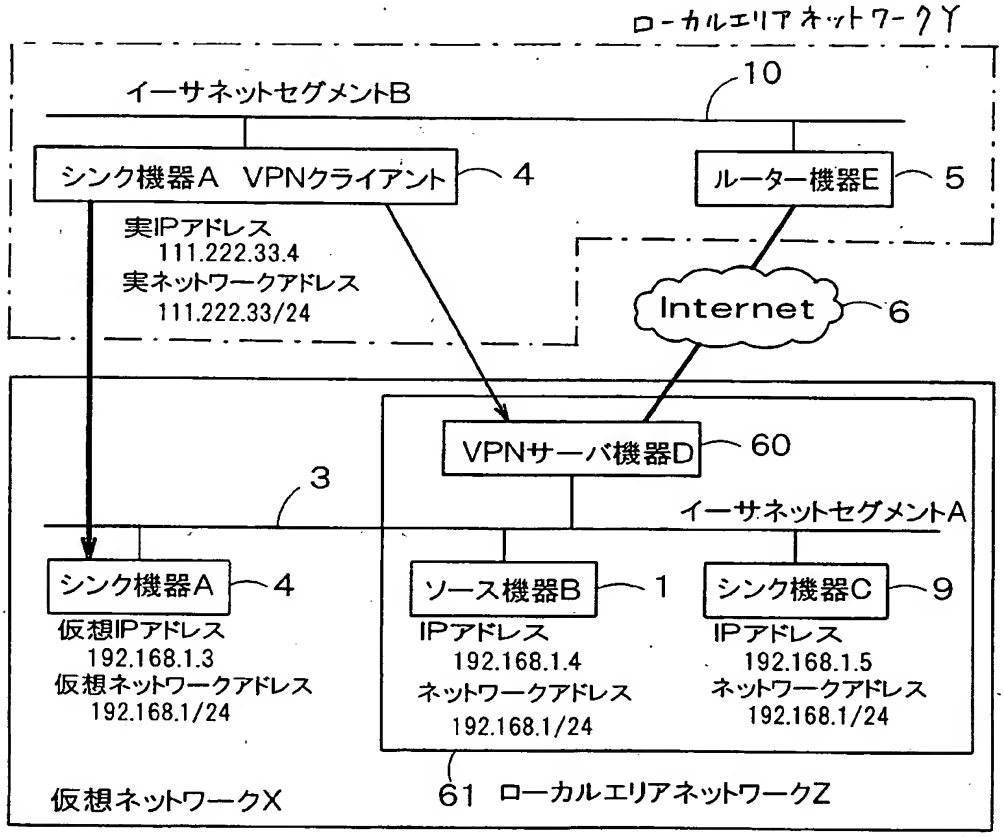
【図３４】


シンク機器E
8
IPアドレス　192.168.2.2
ネットワークアドレス　192.168.2/24
イーサネットセグメントB
5
10
ルーター機器D
シンク機器A
4
IPアドレス　192.168.1.3
ネットワークアドレス　192.168.1/24
イーサネットセグメントA
ソース機器B
1
3
9
シンク機器C
IPアドレス　192.168.1.4
ネットワークアドレス　192.168.1/24
IPアドレス　192.168.1.5
ネットワークアドレス　192.168.1/24

【図３５】


シンク機器のネットワークアドレスAをソース機器に登録
S21
シンク機器はネットワークアドレスAと自ネットワークアドレスを比較
S22
同一の値であるか？
S23
YES
NO
S24
2台の機器は同一のローカルネットワーク　にいると判断
異なるネットワークアドレスであるためコンテンツの送受信処理を中止
S26
TTL＝1でパケットの送信を行う
S25

【図３６】


ローカルエリアネットワークY
イーサネットセグメントB
10
シンク機器A　VPNクライアント
4
ルーター機器E
5
実IPアドレス
111.222.33.4
実ネットワークアドレス
111.222.33/24
Internet
6
VPNサーバ機器D
60
3
イーサネットセグメントA
シンク機器A
4
ソース機器B
1
シンク機器C
9
仮想IPアドレス
192.168.1.3
仮想ネットワークアドレス
192.168.1/24
IPアドレス
192.168.1.4
ネットワークアドレス
192.168.1/24
IPアドレス
192.168.1.5
ネットワークアドレス
192.168.1/24
仮想ネットワークX
61
ローカルエリアネットワークZ

【書類名】　要約書

【要約】

【課題】　限られた受信装置だけにコンテンツを送信可能にする。

【解決手段】　本発明に係るコンテンツ送受信システムは、イーサネットセグメントＡ１０に接続されるシンク機器Ｂ１１、シンク機器Ｂ１２及びルータ機器Ｆ１３と、ルータ機器Ｆ１３にインターネット１４を介して接続されるソース機器Ａ１５とを有する。ソース機器Ｂ５１は同一イーサネットセグメントＡ１０に接続されているシンク機器のみにコンテンツの送受信を許可するため、例えばVPNサーバ機器Ｆ５３を介して接続されるシンク機器等へのコンテンツの送受信を確実に禁止できる。

【選択図】　図１

認定・付加情報

特許出願の番号	特願２００２－３５７１６８
受付番号	５０２０１８６２４２１
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１４年１２月１２日

＜認定情報・付加情報＞

【特許出願人】
- 【識別番号】 000003078
- 【住所又は居所】 東京都港区芝浦一丁目１番１号
- 【氏名又は名称】 株式会社東芝

【代理人】 申請人
- 【識別番号】 100075812
- 【住所又は居所】 東京都千代田区丸の内３－２－３　協和特許法律事務所
- 【氏名又は名称】 吉武　賢次

【選任した代理人】
- 【識別番号】 100088889
- 【住所又は居所】 東京都千代田区丸の内３丁目２番３号　協和特許法律事務所
- 【氏名又は名称】 橘谷　英俊

【選任した代理人】
- 【識別番号】 100082991
- 【住所又は居所】 東京都千代田区丸の内３丁目２番３号　富士ビル協和特許法律事務所
- 【氏名又は名称】 佐藤　泰和

【選任した代理人】
- 【識別番号】 100096921
- 【住所又は居所】 東京都千代田区丸の内３－２－３　富士ビル３階協和特許法律事務所
- 【氏名又は名称】 吉元　弘

【選任した代理人】
- 【識別番号】 100103263
- 【住所又は居所】 東京都千代田区丸の内３丁目２番３号　協和特許法律事務所

次頁有

認定・付加情報（続き）

【氏名又は名称】　川崎　康

次頁無

特願２００２－３５７１６８

出　願　人　履　歴　情　報

識別番号　　［０００００３０７８］

１．変更年月日　　２００１年　７月　２日
［変更理由］　　住所変更
住　所　　東京都港区芝浦一丁目１番１号
氏　名　　株式会社東芝

２．変更年月日　　２００３年　５月　９日
［変更理由］　　名称変更
住所変更
住　所　　東京都港区芝浦一丁目１番１号
氏　名　　株式会社東芝